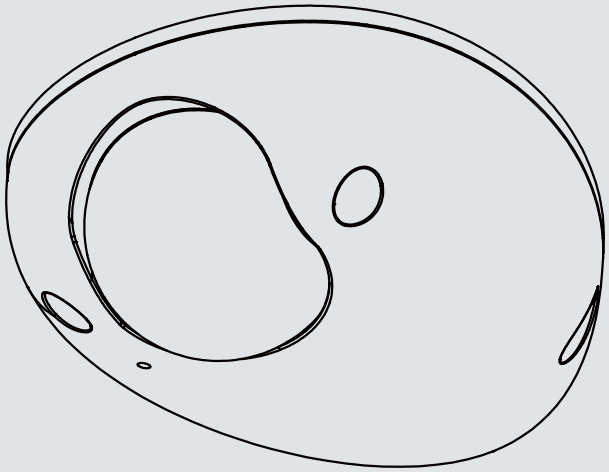
VIVOTEK

MD8531H Mobile Dome Network Camera

User's Manual

1.2MP • Vandal-proof • WDR • Mobile Surveillance



Rev. 1.1

SUPREME

Table of Contents

Overview 4
- Revision History 4
- Read Before Use 5
- Package Contents 5
- Symbols and Statements in this Document 5
- Physical Description 6

Installation 8
- Hardware Installation 8
- Network Deployment 13
- Software Installation 16
- Ready to Use 17
- Adjusting the Lens 18

Accessing the Network Camera 20
- Using Web Browsers 20
- Using RTSP Players 23
- Using 3GPP-compatible Mobile Devices 24
- Using VIVOTEK Recording Software 25

Main Page 26

Client Settings 31

Configuration 35
- System > General settings 36
- System > Homepage layout 38
- System > Logs 41
- System > Parameters 43
- System > Maintenance 44
- Media > Image 48
- Media > Video 55
- Media > Audio 61
- Network > General settings 62
- Network > Streaming protocols 69
- Network > SNMP (Simple Network Management Protocol) 78
- Security > User Account 79
- Security > HTTPS (Hypertext Transfer Protocol over SSL) 81
- Security > Access List 88
- PTZ > PTZ settings 93
- Event > Event settings 97
- Applications > Motion detection 111
- Applications > DI and DO 114
- Applications > Tampering detection 114
- Applications > Temperature detection 115
- Applications > Audio detection 116
- Applications > VADP (VIVOTEK Application Development Platform) 118
- Recording > Recording settings 120
- Local storage > SD card management 125

Local storage > Content management 126
Appendix 129
URL Commands for the Network Camera 129
Technical Specifications 213
Technology License Notice 215
Electromagnetic Compatibility (EMC) 216

Overview

VIVOTEK MD8531H is a compact, 1.2-megapixel network camera geared toward transportation applications such as buses, trains, and other vehicles. With full EN50155 compliance & IP66-rated design, the camera can withstand shock, vibration, humidity, dust, and temperature fluctuations, maintaining stable and reliable video during vehicle movement. Furthermore, the vandal-proof metal housing effectively provides robust protection from vandalism. As such, the combination of high resolution imaging and protective housing endows the MD8531H with the rugged reliability required to maximize passenger safety and optimize mobile surveillance.

With the tamper detection feature, the MD8531H becomes a truly robust and intelligent camera that keeps security staff notified once it suffers video loss from being blocked or spray-painted. PoE (Power-over-Ethernet) also allows the camera to be operated and powered with a single Ethernet cable, giving greater ease of installation. In order to facilitate on-board storage and data portability, the camera is also complete with a MicroSD/SDHC/SDXC card slot for local recording. In corridor scenario, video rotation feature can provide wider vertical coverage for more depth.

Featuring the Wide Dynamic Range Technology WDR Pro, it provides improved visibility in the extremely dark & light environment. Combined with 3D Noise Reduction Technology, which enables the MD8531H to capture clear, polished video under low-light conditions and reduce bandwidth from sensor noise, users can identify an increased level of image details in pretty bright as well as dark environments.

Revision History

Rev. 1.0: Initial release.
Rev. 1.1: Corrected description about PoE connection.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Package Contents

- MD8531H
- Alignment Sticker/Ceiling Hole Template Sticker
- Screws
- Screwdriver
- Desicant Bag
- Software CD
- Quick Installation Guide

Symbols and Statements in this Document

INFORMATION: provides important messages or advices that might help prevent inconvenient or problem situations.

NOTE: Notices provide guidance or advices that are related to the functional integrity of the machine.

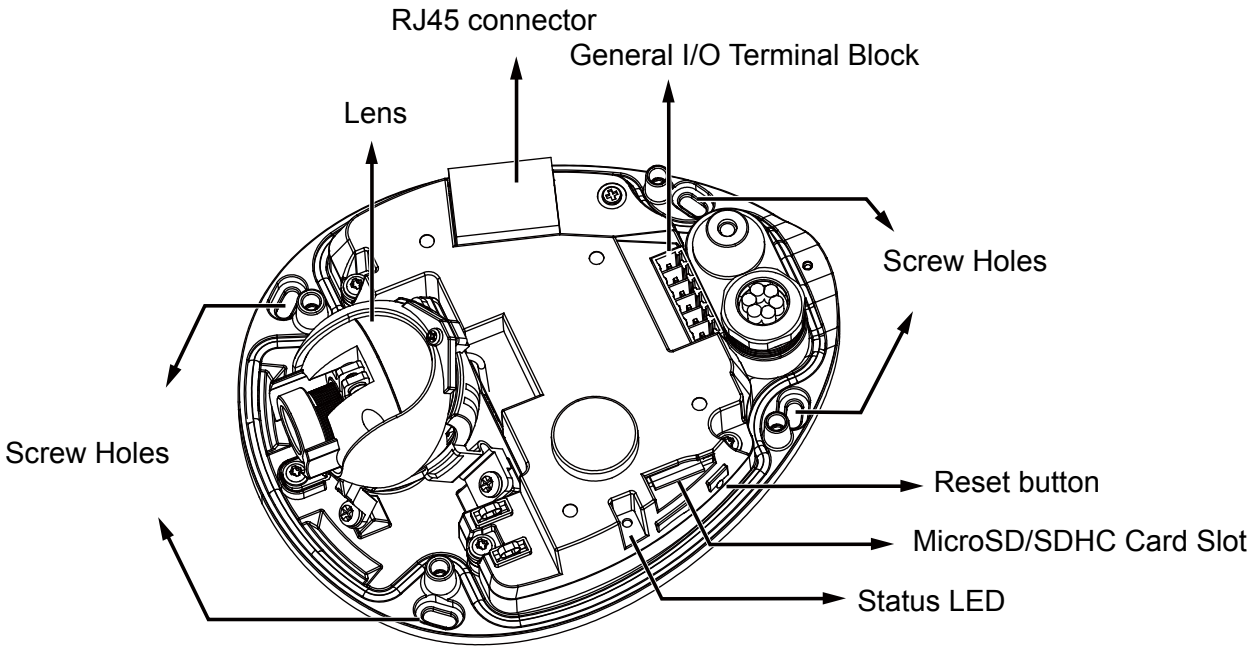
Tips: Tips are useful information that helps enhance or facilitae an installation, function, or process.

WARNING! or IMPORTANT!: These statements indicate situations that can be dangerous or hazardous to the machine or you.

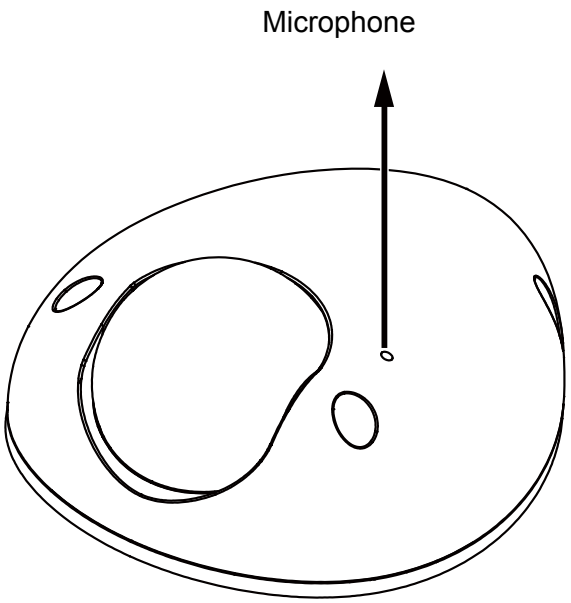
Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

Physical Description

Inner View

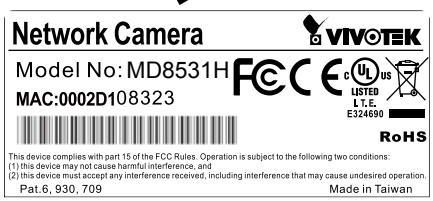


Outer View



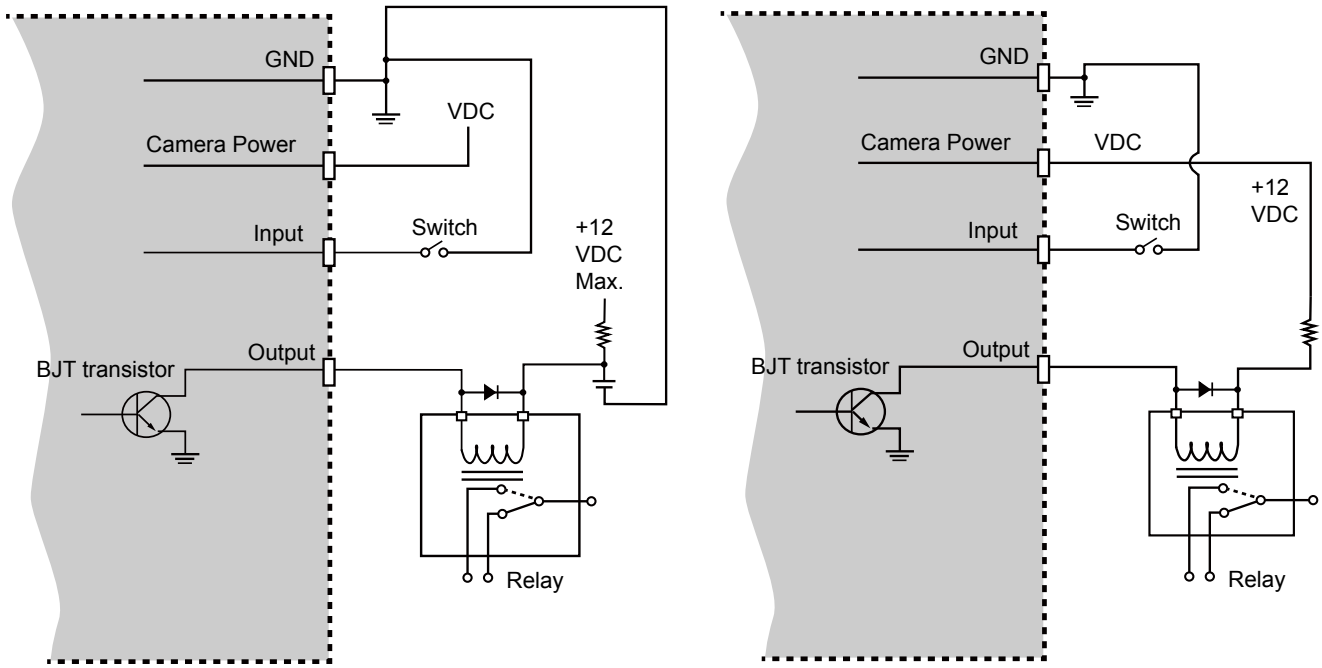
Waterproof Level: IP66

IMPORTANT:
Record the MAC address before installing the camera.

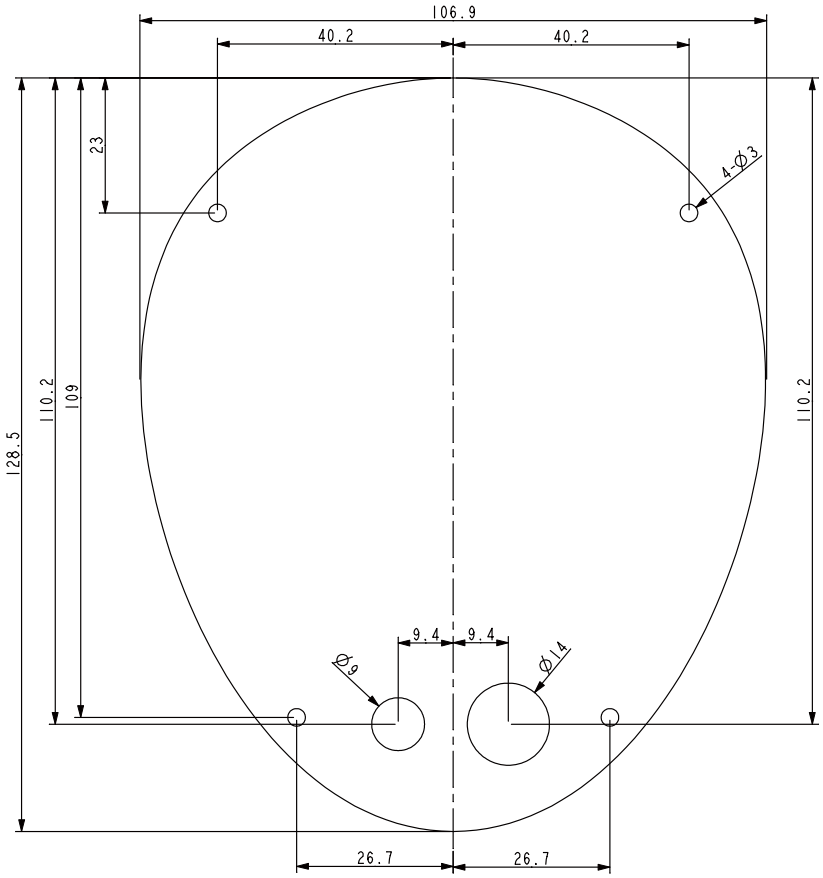


DI/DO Diagram

Please refer to the following illustration for the connection method.



Dimensions

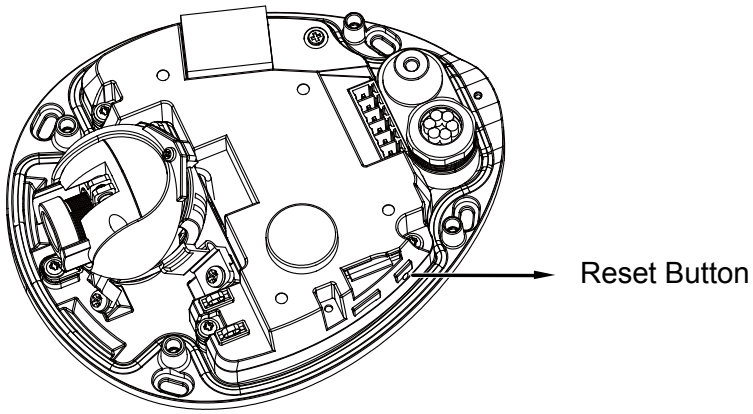


Hardware Reset

The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Reset: Press and release the recessed reset button with a straightened paper clip. Wait for the Network Camera to reboot.

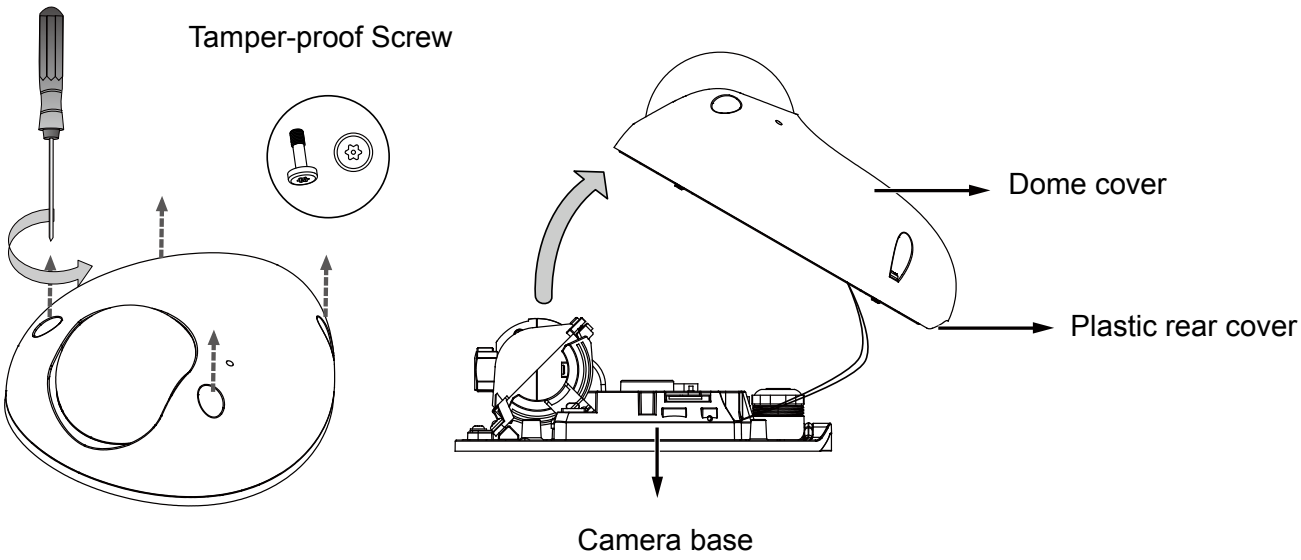
Restore: Press and hold the recessed reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.



Installation

Hardware Installation

First, use the supplied screwdriver to detach the dome cover from the camera base. Insert your MicroSD/ SDHC Card if necessary.

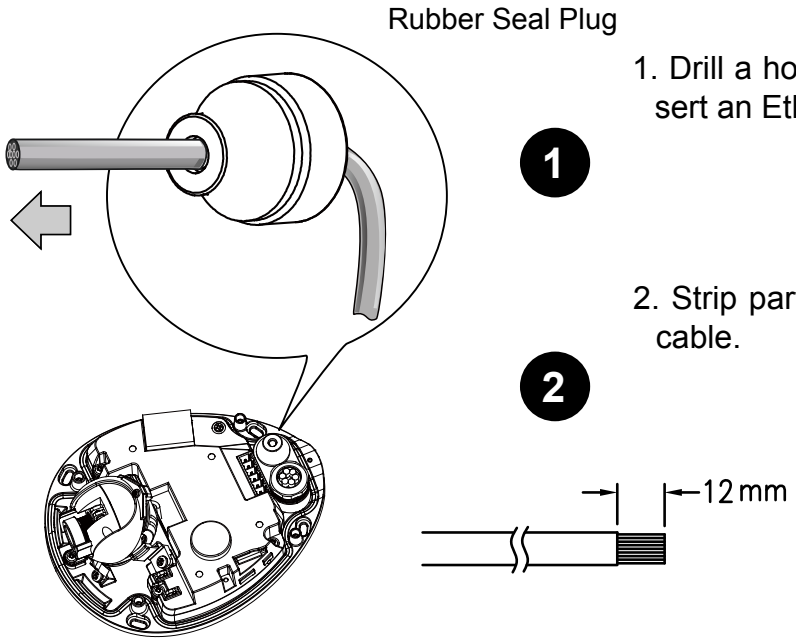


3.1 Connecting RJ45 Ethernet Cable

RJ45 Cable Dimension

Recommended cable diameter: 5 to 8mm (Use CAT5e only)

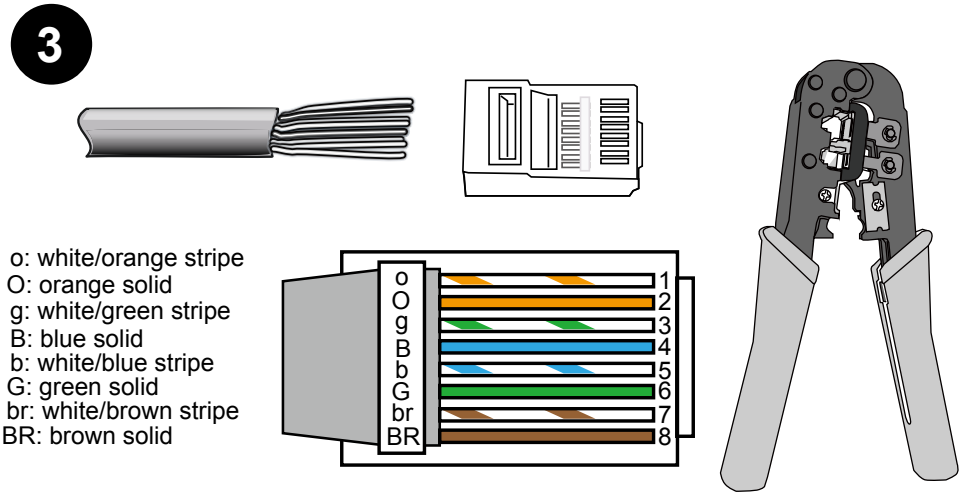
Assembling Steps

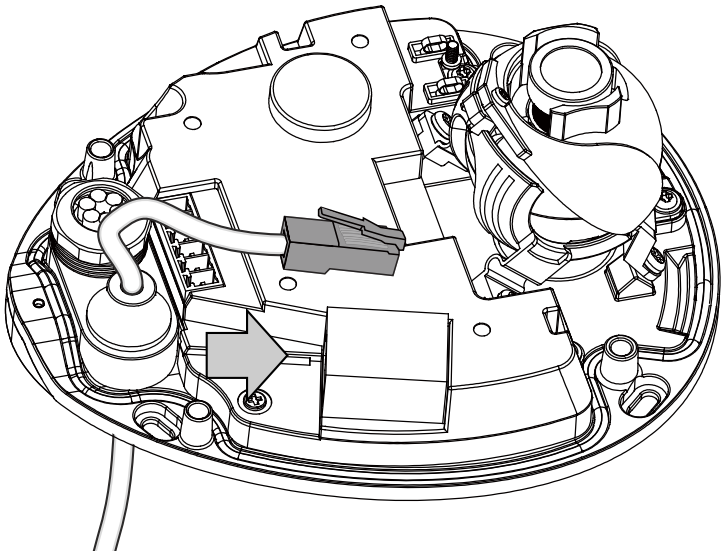


1. Drill a hole on the rubber seal plug and insert an Ethernet cable through the opening.

2. Strip part of the sheath from the Ethernet cable.

3. You will need an RJ45 crimping tool to attach the Ethernet wires to a connector. When done, connect the cable to the camera's Ethernet RJ45 socket.

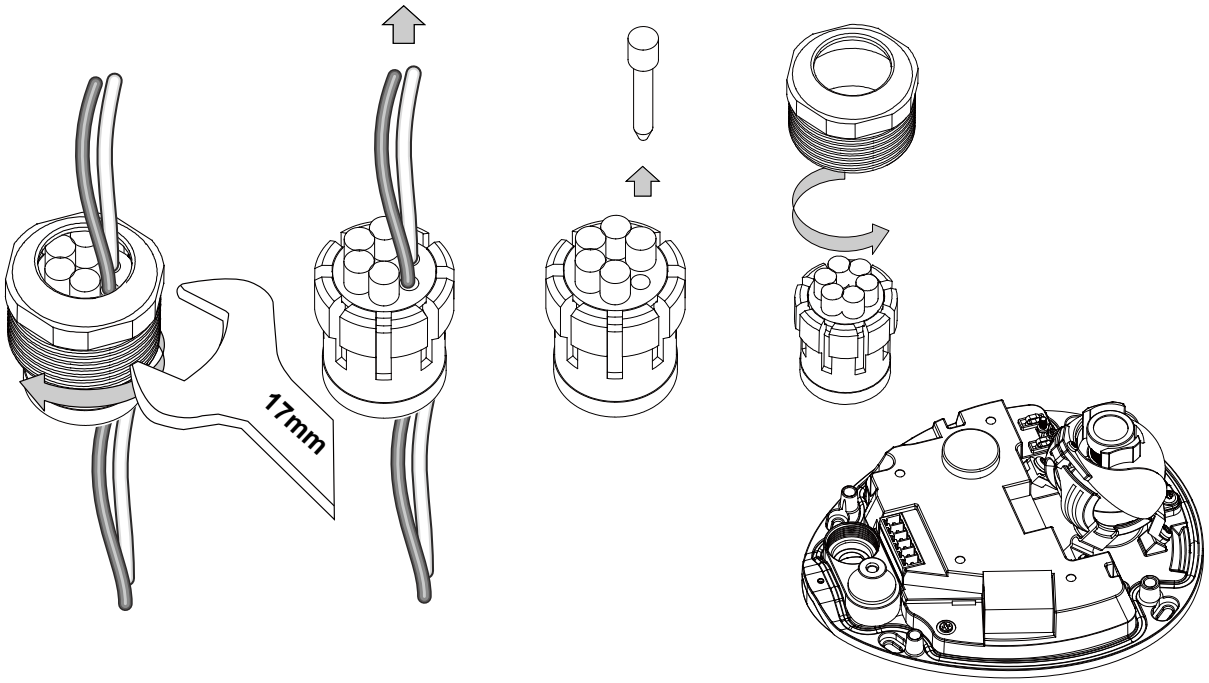




3.2 Connecting IO cables:

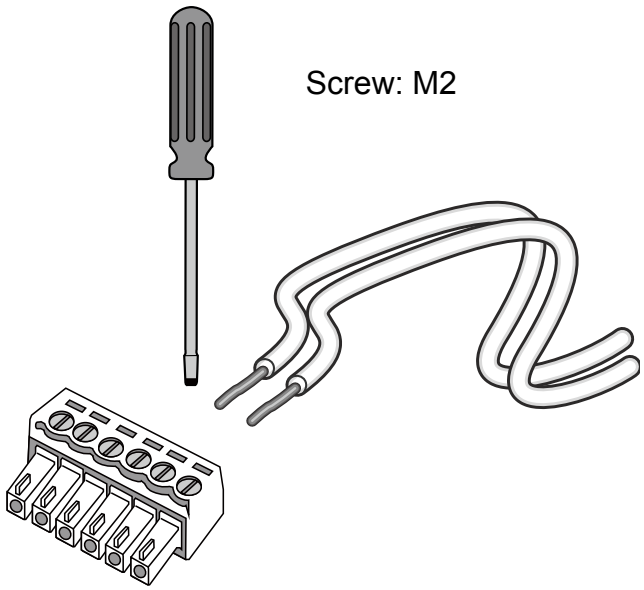
1. Remove the waterproof connector from the camera, and pass IO wires through the rubber seal as shown below. Tighten up and install the connector when done.

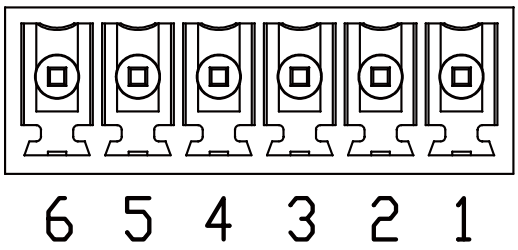
   Wire range: 1.5mm~1.8mm; 20AWG
   Strip length: 6~7mm



2. Use a small-size flat-blade screwdriver to secure IO wires to the included terminal blocks.

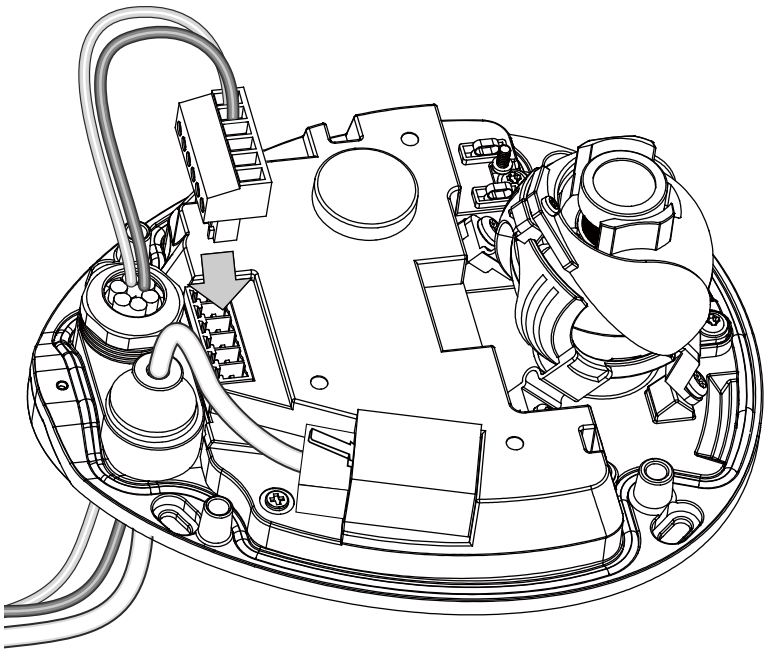
   The pinouts are shown below.





1	DI-
2	DI+
3	DO-
4	DO+
5	Audio GND
6	Audio Out

3. Connect the terminal block to the camera.



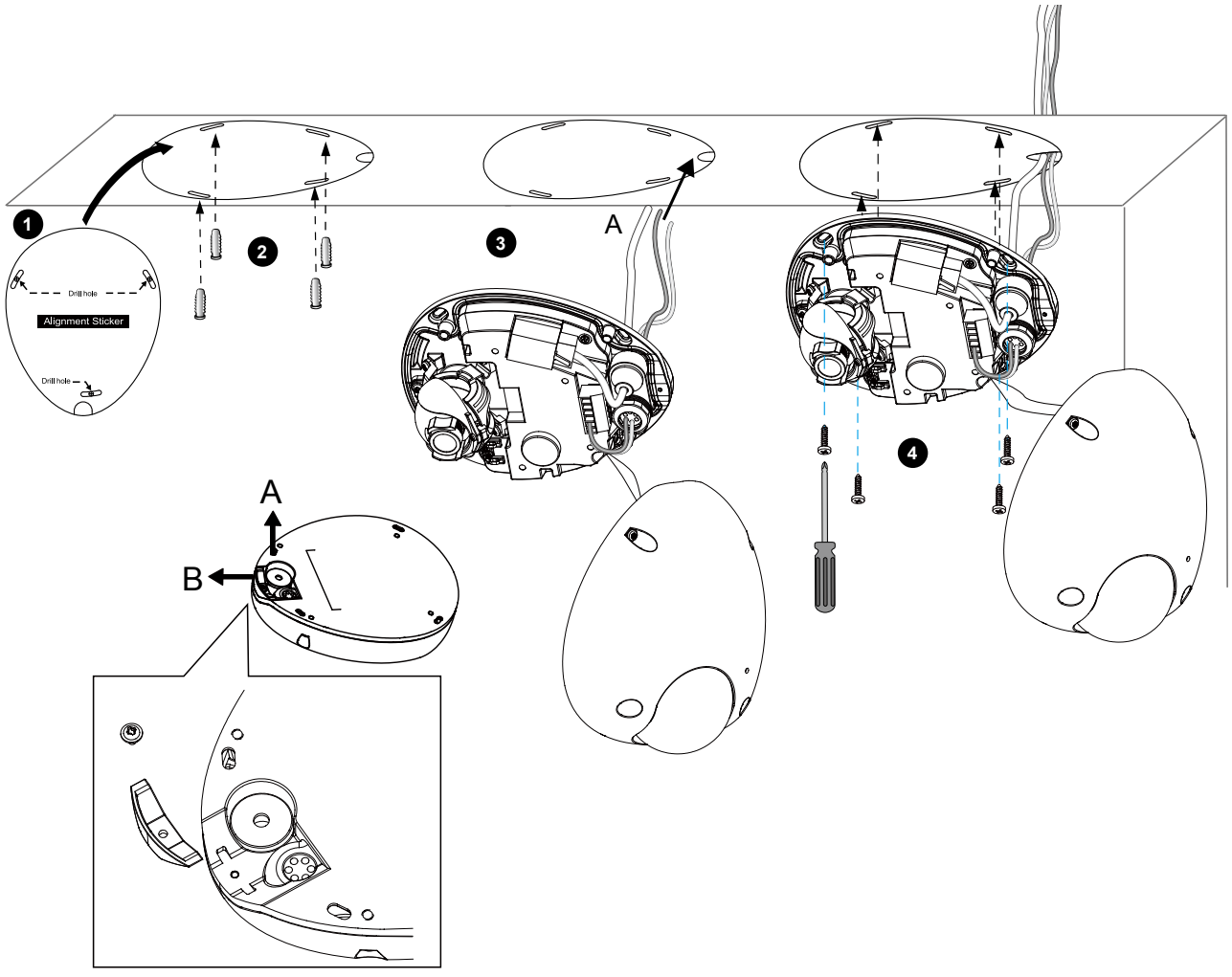
NOTE:

1. This equipment is only to be connected to PoE networks without routing to outside plants.
2. For PoE input connection, use only UL listed I.T.E. with PoE output.

3.3 Ceiling Mount

Then, follow the steps below to install the camera to either a ceiling or wall:

1. Attach the supplied alignment sticker to the ceiling/wall.
2. Using the 4 screw circles on the sticker, drill 4 pilot holes into the ceiling/wall. Then hammer the plastic anchors into the holes if necessary.
3. This Network Camera can be mounted with the cable routed through the ceiling/wall or from the side. If you want to feed the cable through the ceiling/wall, drill a cable hole A as shown in the picture. If the cable goes through the rear opening of the dome cover, please remove the plastic cover (B).
4. Through the 4 holes on the camera base, insert the screws to corresponding holes and secure the camera base with a screwdriver.

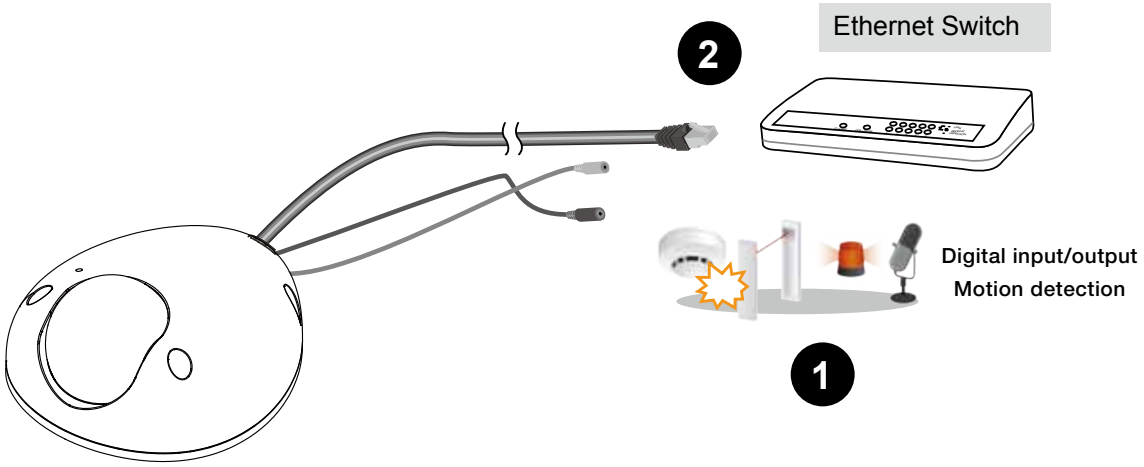


Network Deployment

Setting up the Network Camera over the Internet

General Connection (with PoE)

1. If you have external devices such as sensors and alarms, connect them to the general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.



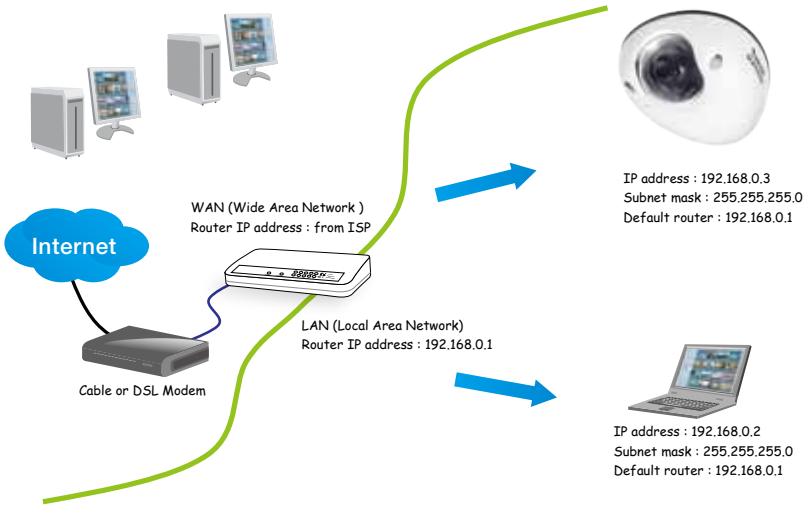
IMPORTANT:

The product should not be connected to an Ethernet network with outside plant routing. The ITE is to be connected only to PoE networks without routing to the outside plant.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 16 for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

   - HTTP port: default is 80
   - RTSP port: default is 554
   - RTP port for audio: default is 5558
   - RTCP port for audio: default is 5559
   - RTP port for video: default is 5556
   - RTCP port for video: default is 5557

   If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 62 for details.

For example, your router and IP settings may look like this:

Device	IP Address: internal port	IP Address: External Port (Mapped port on the router)
Public IP of router	122.146.57.120	
LAN IP of router	192.168.2.1	
Camera 1	192.168.2.10:80	122.146.57.120:8000
Camera 2	192.168.2.11:80	122.146.57.120:8001
...	...	...

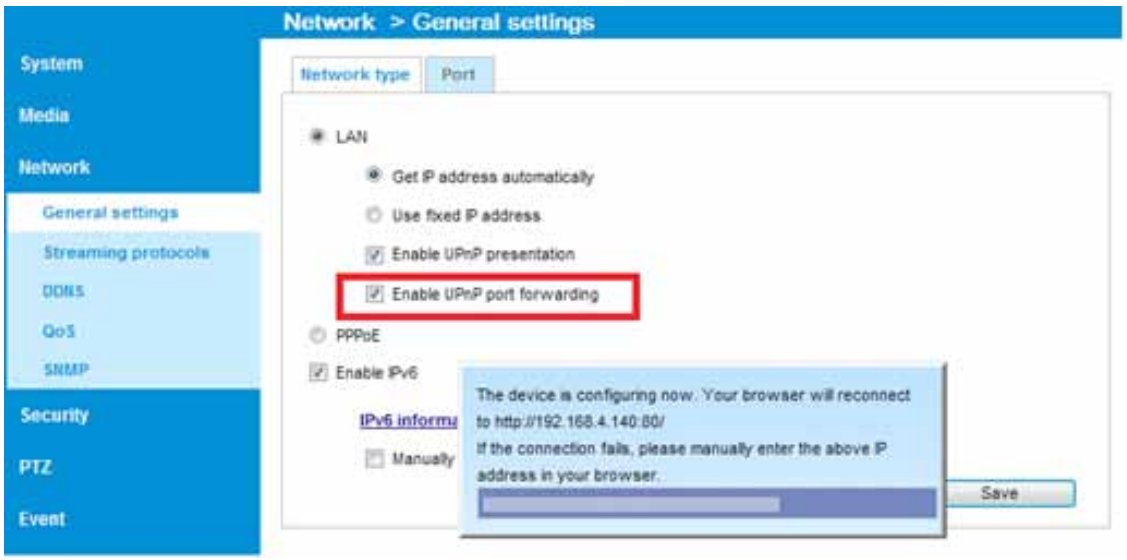
Configure the router, virtual server or firewall, so that the router can forward any data coming into a preconfigured port number to a network camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80
...	...

When properly configured, you can access a camera behind the router using the HTTP request as follows: http://122.146.57.120:8000

If you change the port numbers on the Network configuration page, please open the ports accordingly on your router. For example, you can open a management session with your router to configure access through the router to the camera within your local network. Please consult your network administrator for router configuration if you have troubles with the configuration.

For more information with network configuration options (such as that of streaming ports), please refer to Configuration > Network Settings. VIVOTEK also provides the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.



Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN setting on page 62 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 63 for details.

Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

1. Install IW2 under the Software Utility directory from the software CD. Double-click the IW2 shortcut on your desktop to launch the program.

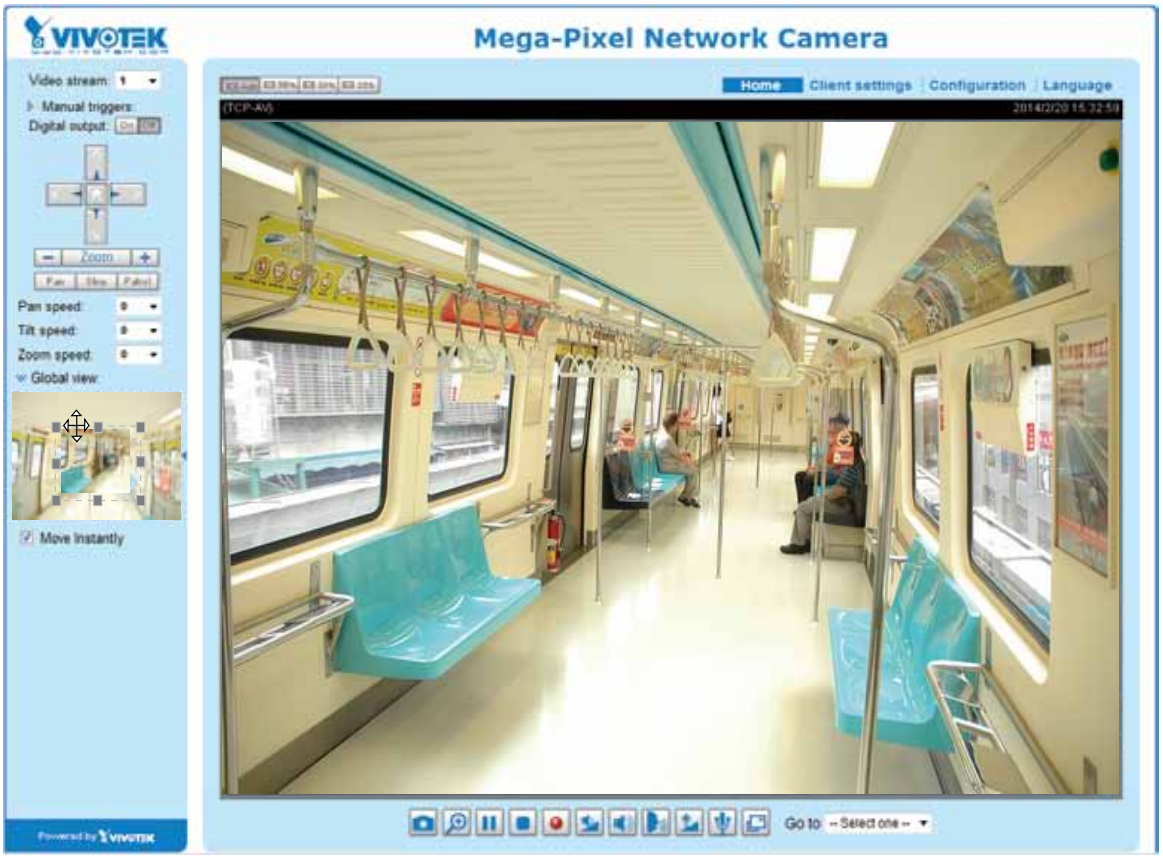
2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.

3. The program will search for all VIVOTEK network devices on the same LAN.

4. After a brief search, the installer window will prompt. Click on the MAC and model name that matches the one printed on the product label. You can then double-click on the address to open a management session with the Network Camera.

Ready to Use

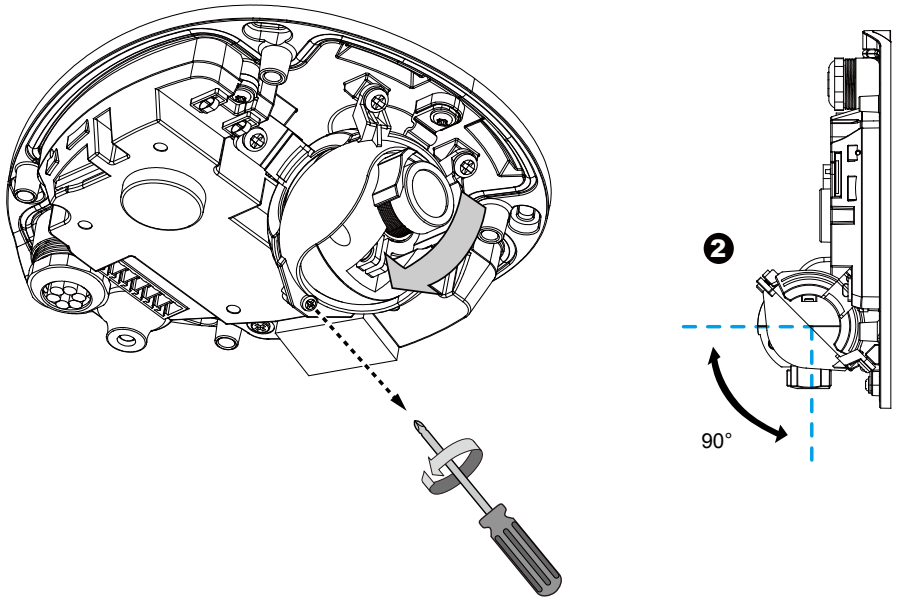
1. A browser session with the Network Camera should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.



Adjusting the Lens

To adjust the viewing angle

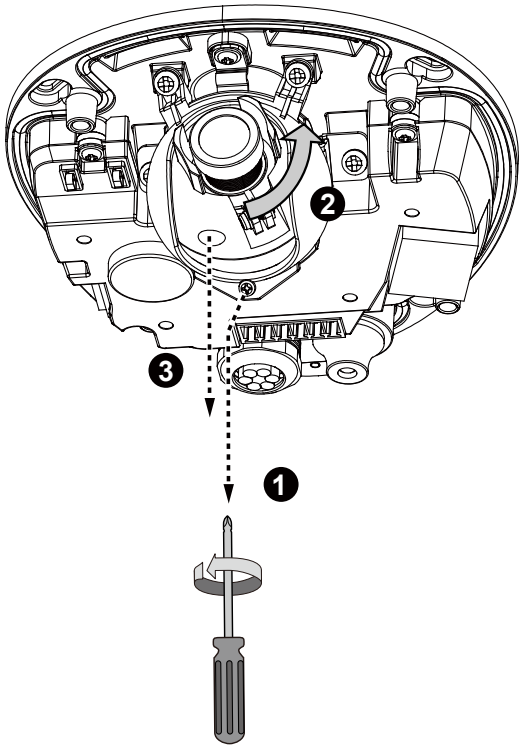
1. Loosen the lens module retention screw (not removing it) on top of the lens module.
2. Adjust the lens to a desired viewing angle.
3. When done, fasten the screw so that lens orientation can be fixed and withstand shock and vibration.



Fine-tune the Camera Focus

The focus of this network camera is set from 1.0 meter to infinity by factory default. If you want to focus on objects closer than 1.0m or the lens has lost focus, please fine tune it in the following way.

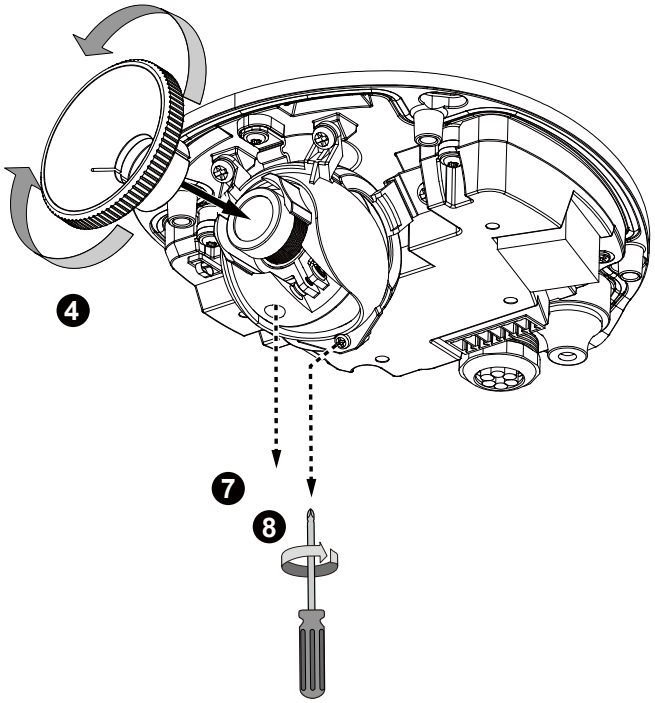
1. Loosen the retention scew on top of the lens module.
2. Rotate the lens module to the side to access the lens focus retention screw.
3. Loosen the focus retentation screw.



NOTE:

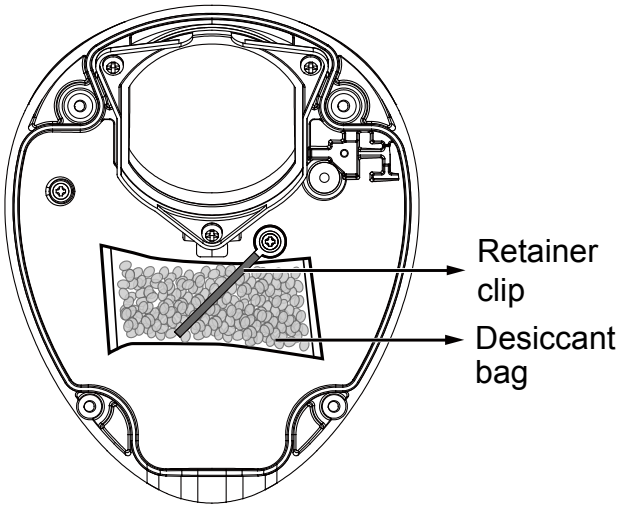
You can also rotate the lens module to correct the field of view when mounted on a tilted surface.

4. Use the adjustment tool to adjust the lens focus by rotating the lens clockwise or counter-clockwise.
5. Rotate the lens module back to the correct orientation. Put on the dome cover, but do not completely tighten its screws yet.
6. Check the live console to see if the image is clear. Repeat the process until the live image is clear.
7. Tighten the lens focus retention screw.
8. Tighten the lens module retention screw.



Completion

Open the aluminum foil vacuum bag and take out the desiccant bag. Attach the supplied desiccant bag to the inner side of the dome cover, to under the retainer clip. (Please replace the desiccant whenever you open the dome cover.)



Attach the dome cover to camera. Secure the dome screws with the supplied screwdriver. Finally, make sure all parts of the camera are securely installed.

IMPORTANT:
Please secure the screws tightly to avoid moisture.

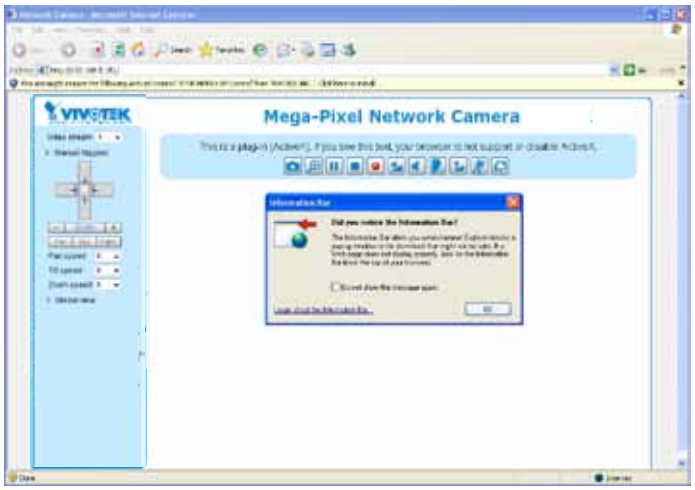
Accessing the Network Camera

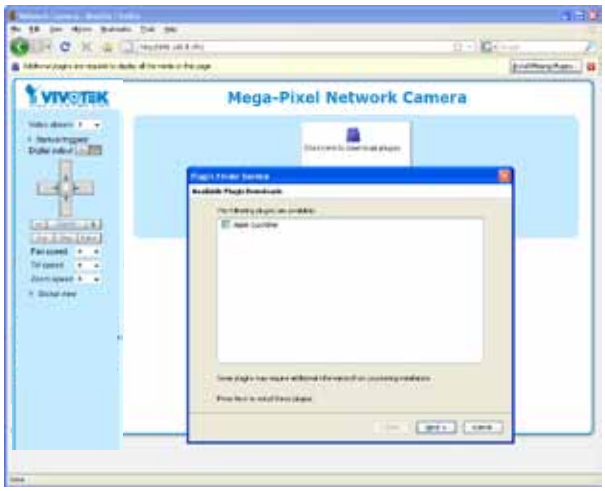
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access the Network Cameras on LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:

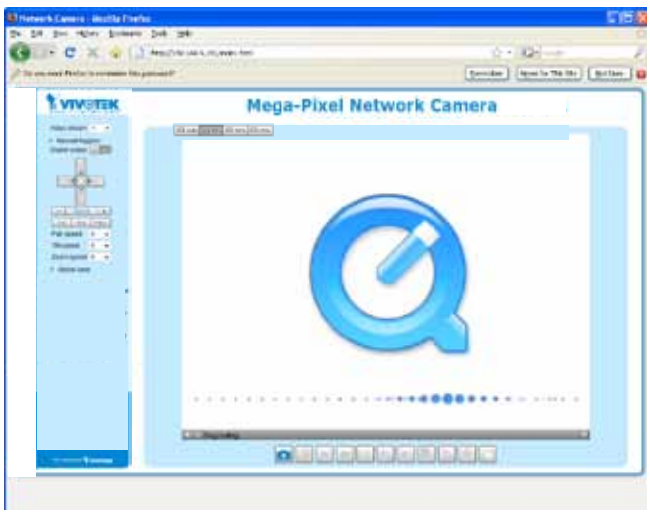
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Google Chrome).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.





NOTE:

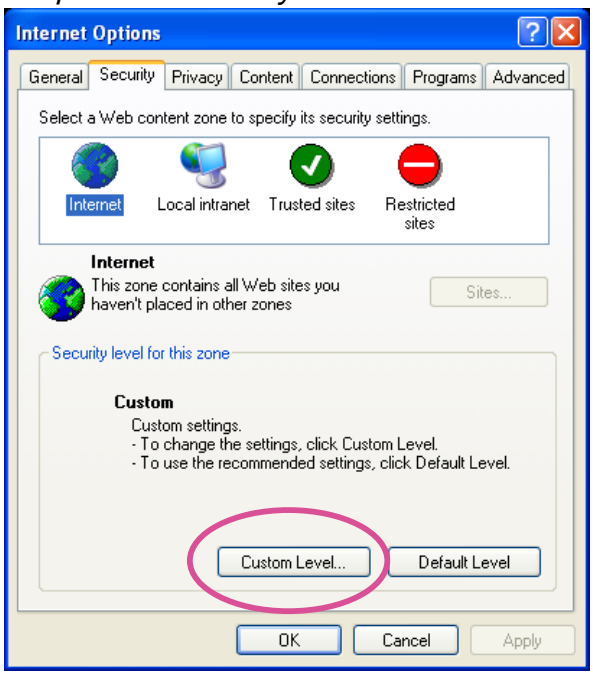
► *For Mozilla Firefox or Google Chrome users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.*



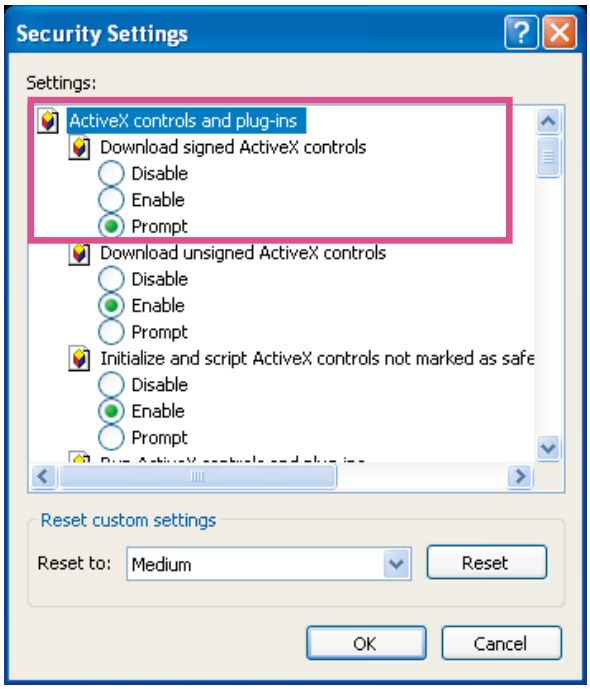
► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 79.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



*2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.*



3. Refresh your web browser, then install the ActiveX® control. Follow the instructions to complete installation.

IMPORTANT:

1. Currently the Network Camera utilizes 32-bit ActiveX plugin. You CAN NOT open a management/view session with the camera using a 64-bit IE browser.
2. If you encounter this problem, try execute the Iexplore.exe program from C:\Windows\SysWOW64. A 32-bit version of IE browser will be installed.
3. On Windows 7, the 32-bit explorer browser can be accessed from here:
   C:\Program Files (x86)\Internet Explorer\iexplore.exe

NOTE:

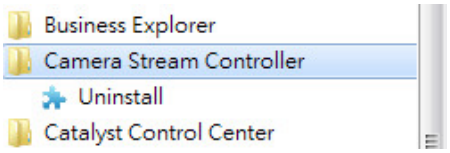
1. For a megapixel camera, it is recommended to use monitors of the 24" size or larger, and capable of 1600x1200 or better resolutions.
2. Below are the defaults for Audio settings:
   For cameras with built-in microphone: **Not Muted.**
   For cameras without built-in microphone: **Muted.**

   To receive audio input from external microphone, you may need to enable the audio input from **Media** > **Audio**. Refer to page 61 for more information.

Tips:

- The onscreen Java control can malfunction under the following situations:

  A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions). Removing your browser cookies will solve this problem.
- In the event of plug-in compatibility issues, you may try to uninstall the plug-in that was previously installed.



Using RTSP Players

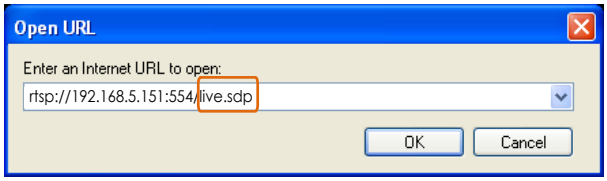
To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

VLC Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream #1, #2, #3, or #4>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 70.
For example:



4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 70 for details.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 14.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 71.

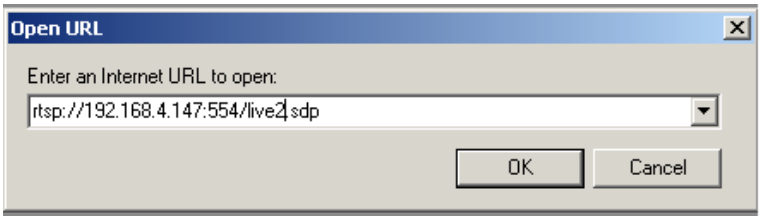
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Stream settings on page 55.

Video Mode	H.264
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (G.711)	PCMU

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 70.

4. Launch the player on the 3GPP-compatible mobile devices (e.g., VLC Player).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream # with small frame size and frame rate>.
   For example:



Using VIVOTEK Recording Software

The product software CD also contains an ST-7501 recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.

VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 36.

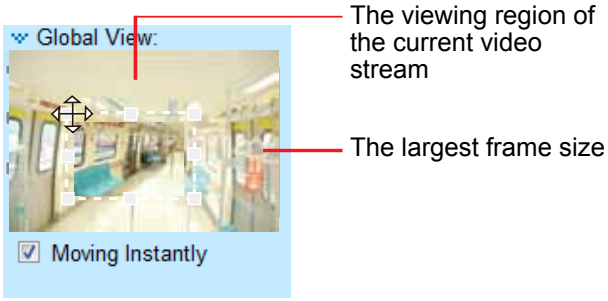
Camera Control Area

Video Stream: This Network Camera supports multiple streams simultaneously. You can select any one for live viewing. For more information about multiple streams, please refer to page 55 for detailed information.

Manual Trigger: Click to enable/disable an event trigger manually. Please configure an event setting on Application page before enable this function. A total of 3 event settings can be configured. For more information about event setting, please refer to page 96. If you want to hide this item on the homepage, please go to **Configuration> System > Homepage Layout > General settings > Customized button** to deselect “show manual trigger button”.

Digital Output: Click to turn the digital output signal on or off.

Global View: Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the current video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation, please refer to E-PTZ Operation on page 93. For more information about how to set up the viewing region of the current video stream, please refer to page 60.



PTZ Panel: This Network Camera supports “digital“ (e-PTZ) pan/tilt/zoom control. Please refer to PTZ settiings on page 93 for detailed information.

Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 31.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 35.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文. Please note that you can also change a language on the Configuration page; please refer to page 35.

Hide Button

You can click the hide button to hide the control panel or display the control panel.

Resize Buttons

:

Click the Auto button, the video cell will resize automatically to fit the monitor.
Click 100% is to display the original homepage size.
Click 50% is to resize the homepage to 50% of its original size.
Click 25% is to resize the homepage to 25% of its original size.

Live Video Window

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:

Video Title: The video title can be configured. For more information, please refer to Video Settings on page 48.

H.264 / MPEG-4 Protocol and Media Options: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 31.

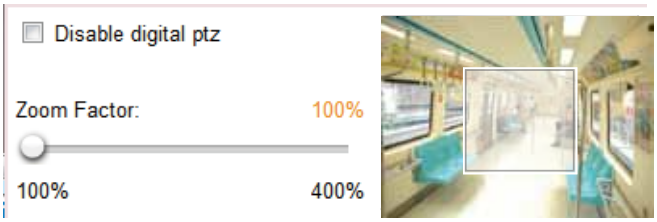
Time: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 48.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 48.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Pause: Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 32 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Media > Image on page 48.

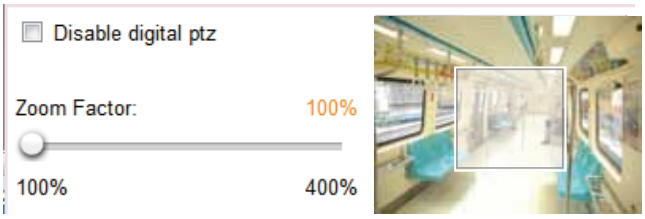
Time: Display the current time. For more information, please refer to Media > Image on page 48.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 48.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 32 for details.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

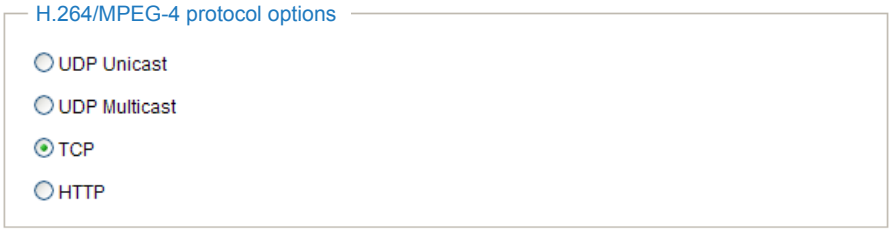
Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264/MPEG-4 Media Options

Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

H.264/MPEG-4 Protocol Options



Depending on your network environment, there are four transmission modes of H.264 or MPEG-4 streaming:

UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 70.

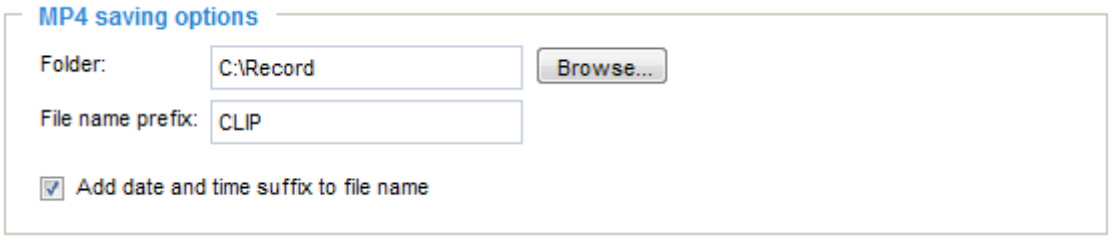
TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

Two way audio

Select one of the checkboxes to configure the two way audio into the half- or full-duplex mode.

MP4 Saving Options

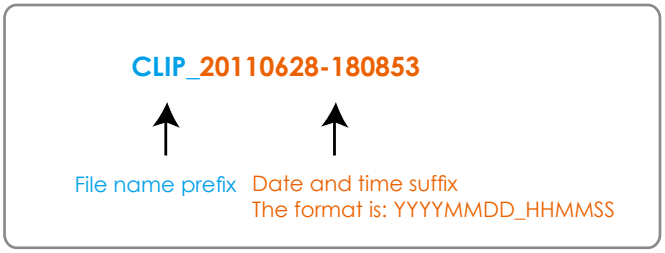


Users can record live video as they are watching it by clicking Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

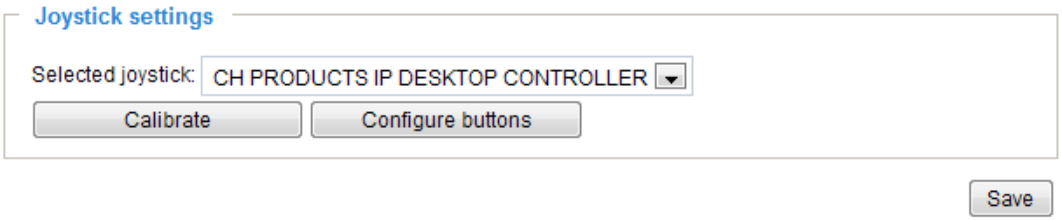
Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.



Local Streaming Buffer Time

In a busy network, fluctuations in available bandwidth can occur. Video streaming may lag and may not proceed very smoothly. If you enable this option, video streams from the camera will be temporarily stored on the computer's cache memory for a configurable period of time (seconds or milliseconds) before being played on a web session. This will help you see the streaming more smoothly. If you enter 3000 Millisecond, the streaming will delay for 3 seconds.

Joystick Settings



Enable Joystick

Connect to the USB plug of the joystick to a USB port on your management computer. Supported by the plug-in in the main page (Microsoft's DirectX), once the plug-in in the main page is loaded, it will automatically detect if there is any joystick on the computer. The joystick should work properly without installing any other driver or software.

Then you can begin to configure the joystick settings of connected devices. Please follow the instructions below to enable joystick settings.

1. Right-click on a live view window. Select Joystick Settings. If your joystick is working properly, it will be displayed on the drop-down list.
2. Select the joystick you want to configure. Check **Enable Joystick**, then click **Configure Buttons** to open Buttons configuration window.

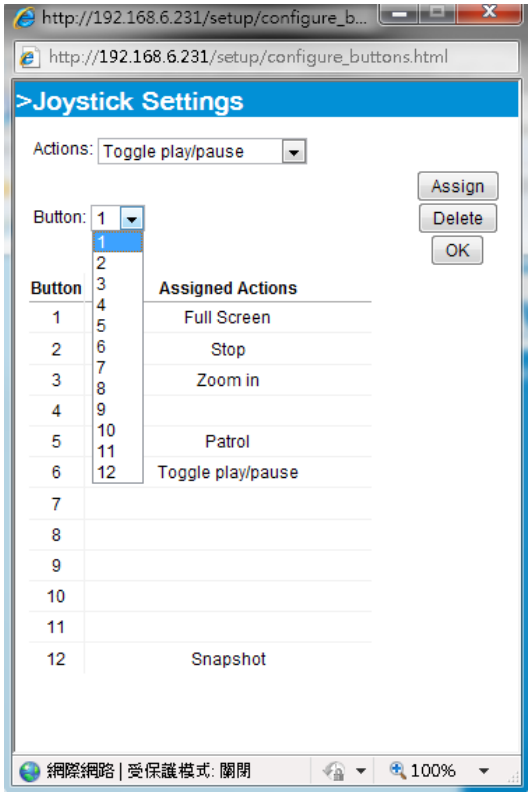
NOTE:

- If you want to assign Preset actions to your joystick, the preset locations should be configured in advance in the Configuration > PTZ page.
- If your joystick is not working properly, it may need to be calibrated. Click the **Calibrate** button to open the Game Controllers window located in Microsoft Windows control panel and follow the instructions for trouble shooting.
- The joystick will appear in the **Game Controllers** list in the Windows Control panel. If you want to check out for your devices, go to the following page: Start -> Control Panel -> Game Controllers.

Buttons Configuration

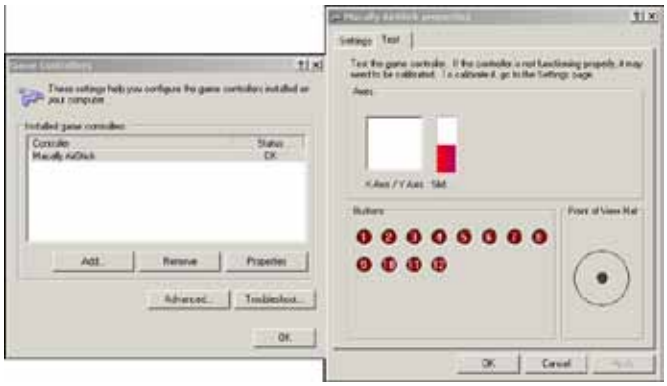
Click the **Configure Buttons** button, a window will prompt as shown below. Please follow the steps below to configure your joystick buttons:

1. Select a button number from the Button # pull-down menu.



Tips:

If you are not sure of the locations of each button, use the **Properties** window in the **Game Controllers** utility.



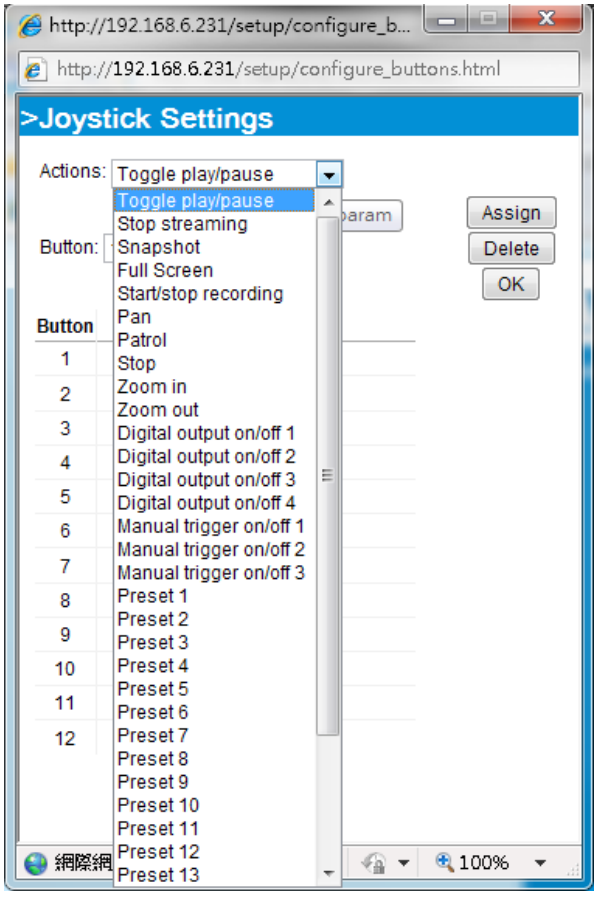
2. Select a corresponding action, such as Patrol or Preset#.

3. Click the **Assign** button to assign an action to the button. You can delete an association by selecting a button number, and then click the **Delete** button.

   Repeat the process until you are done with the configuration of all preferred actions.

   The buttons you define should appear on the button list accordingly.

4. Please remember to click the **Save** button on the Client settings page to preserver your settings.

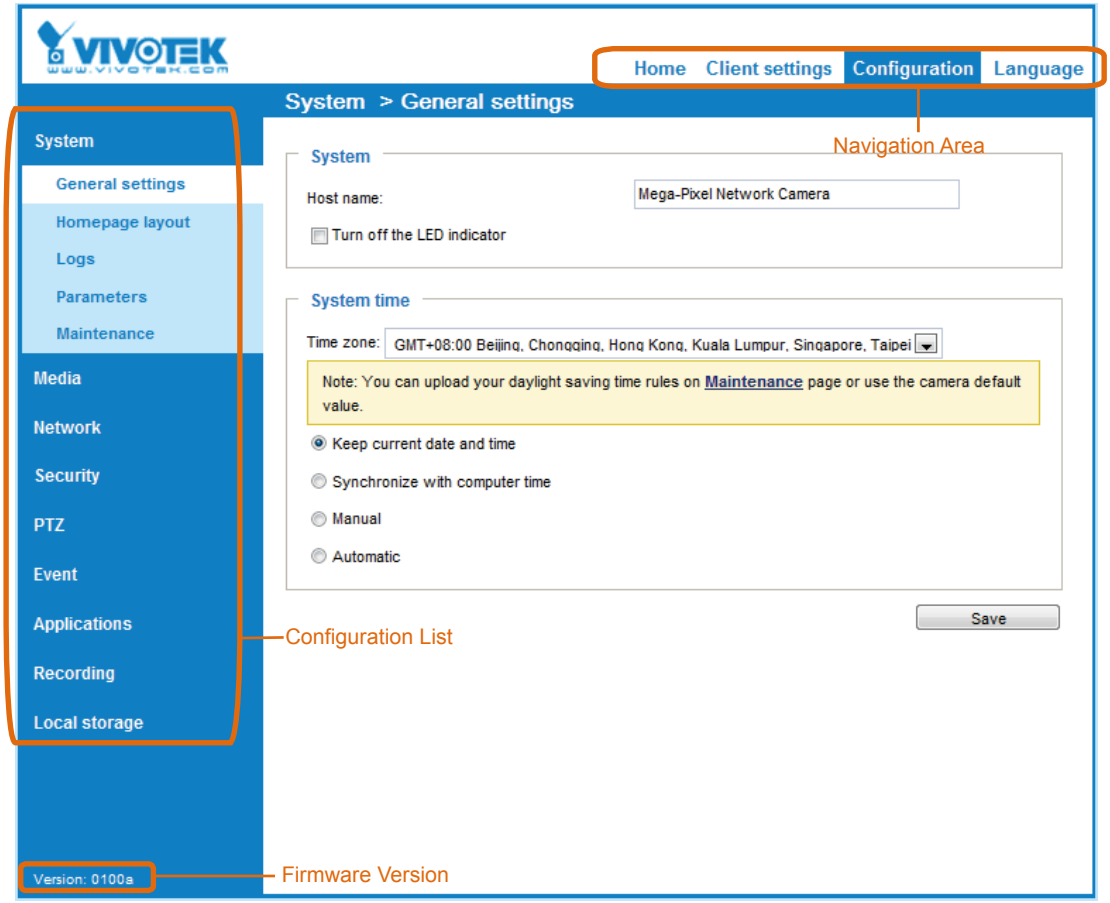


Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

VIVOTEK provides an easy-to-use user interface that helps you set up your network camera with minimal effort. In order to simplify the user interface, detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the main page:



Each function on the configuration list will be explained in the following sections.

The Navigation Area provides access to all different views from the **Home** page (for live viewing), **Configuration** page, and multi-language selection.

System > General settings

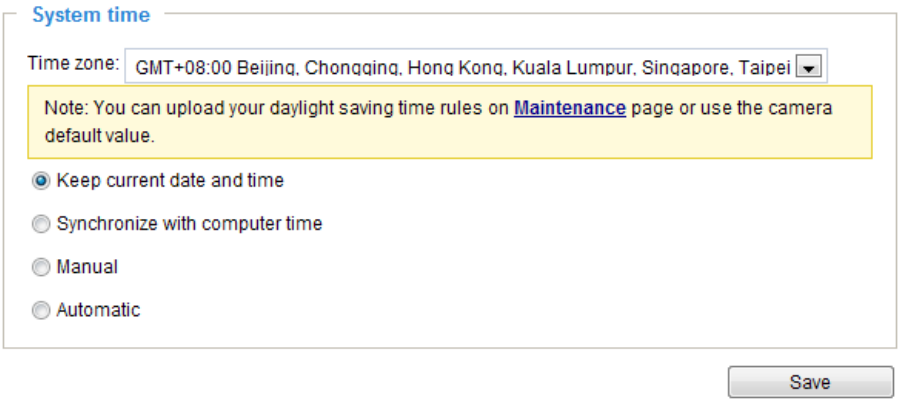
This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System, and System Time. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page, and also on the view cell of ST-7501 and VAST management software.

Turn off the LED indicators: If you do not want others to notice the network camera is in operation, you can select this option to turn off the LED indicators.

System time



Time zone : Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 45 for details.

Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Synchronize with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

System > Homepage layout Advanced Mode

This section explains how to set up your own customized homepage layout.

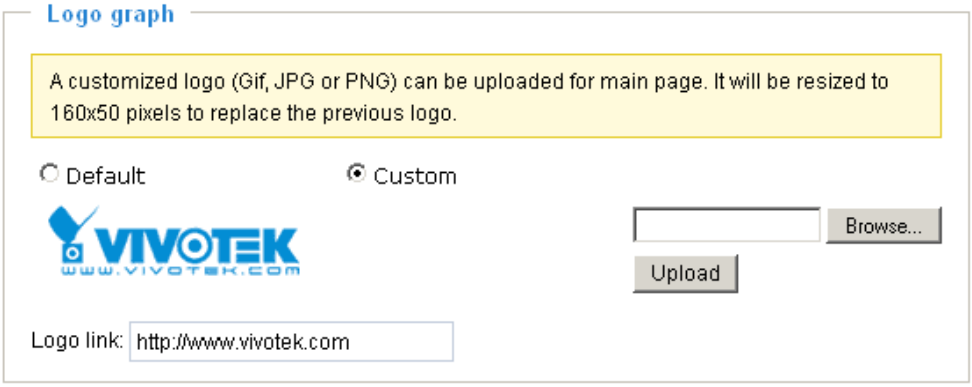
General settings

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo graph

Here you can change the logo at the top of your homepage.



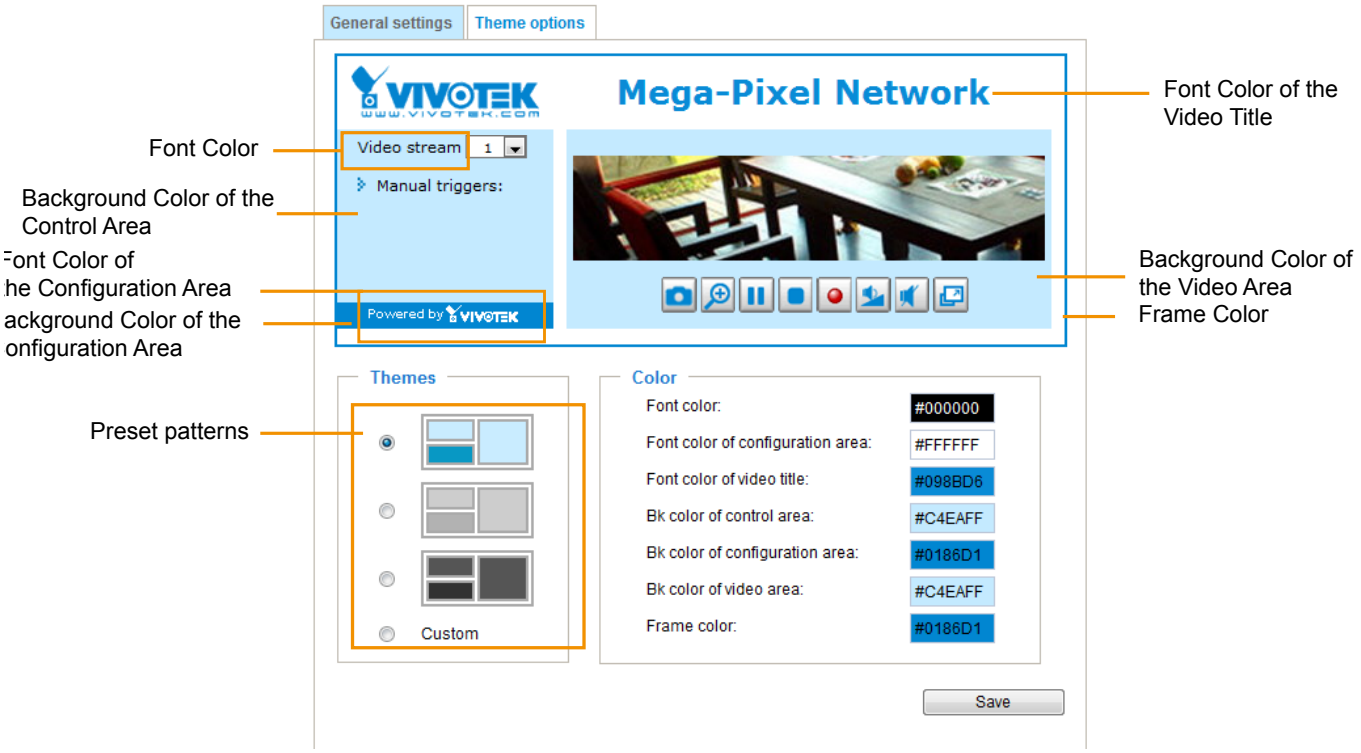
Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Customized button

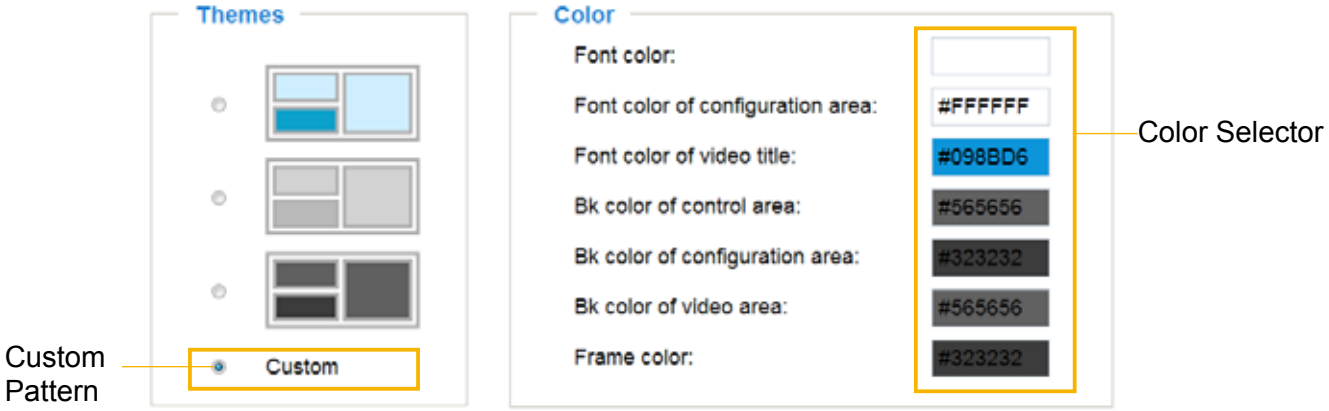
If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is selected by default.

Theme Options

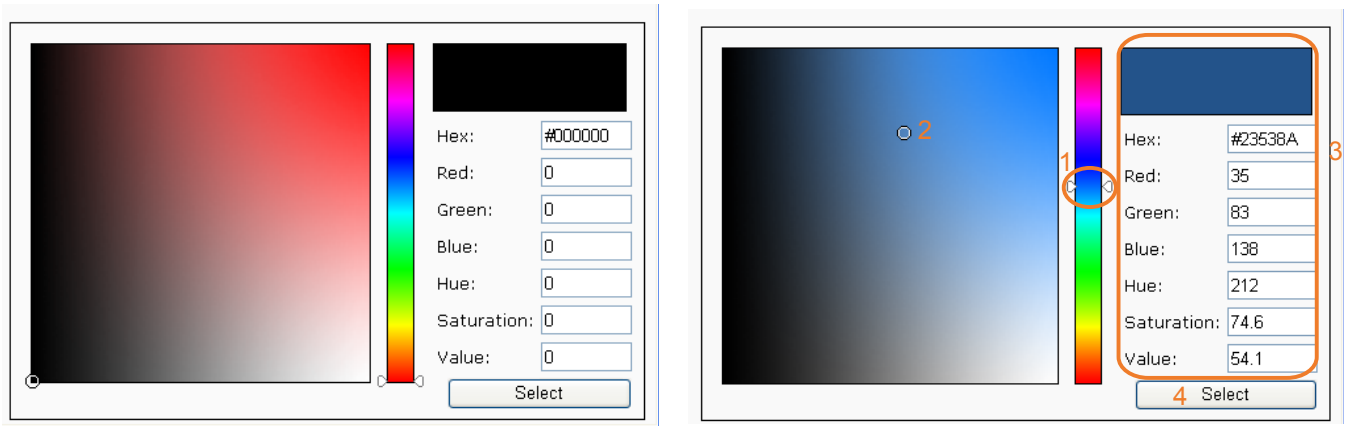
Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



■ Follow the steps below to set up the customed homepage:
1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



3. The palette window will pop up as shown below.



4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

System > Logs Advanced Mode

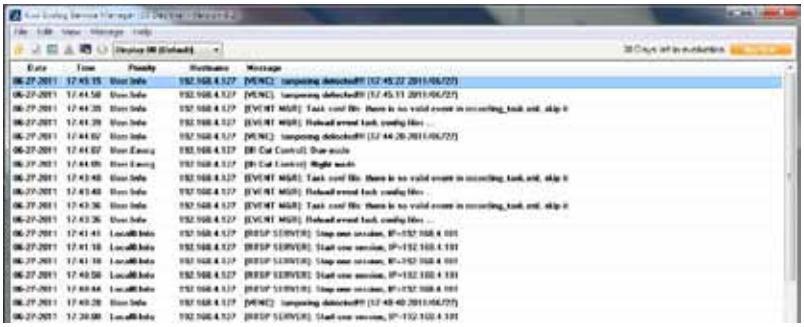
This section explains how to configure the Network Camera to send the system log to a remote server as backup.

Log server settings

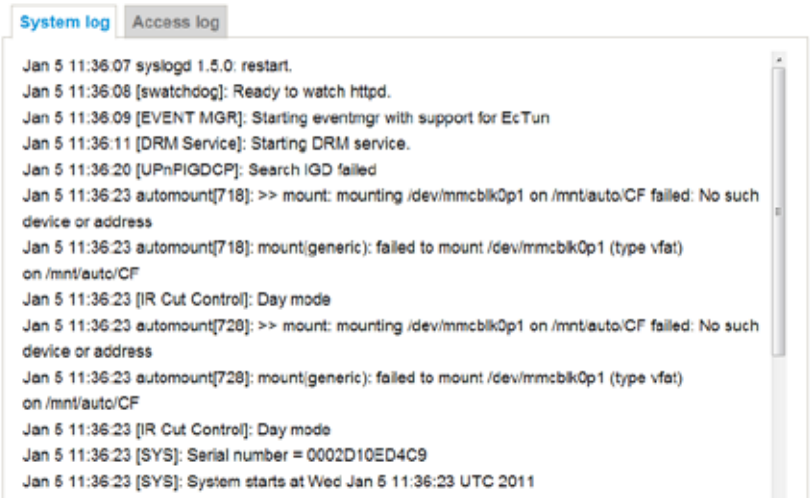
Follow the steps below to set up the remote log:

1. Select **Enable remote log**.
2. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, click **Save** to enable the setting.

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

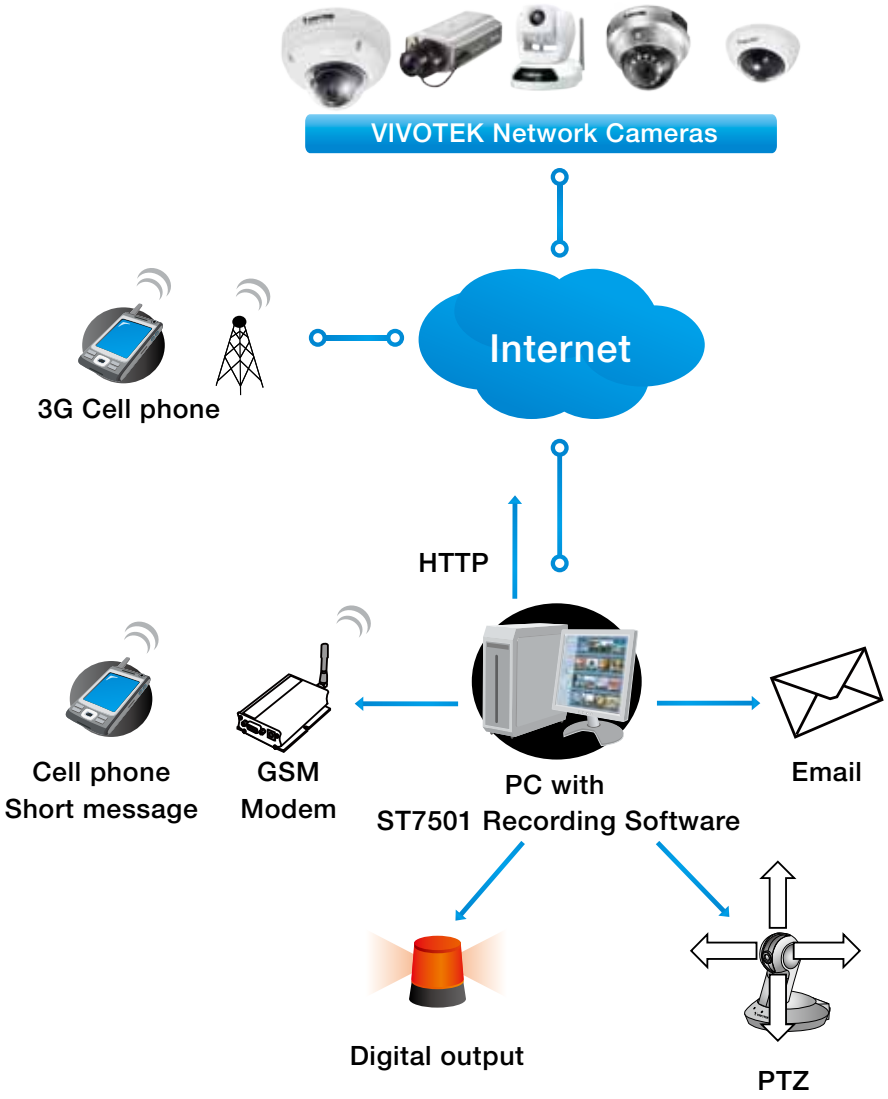


System log

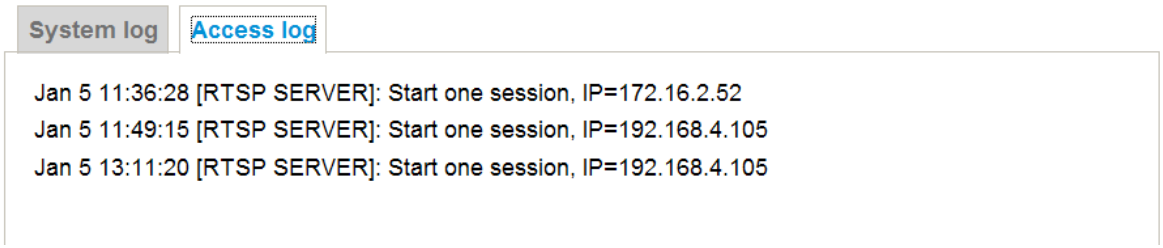


This column displays the system log in a chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

You can install the included ST7501 recording software, which provides an Event Management function group for delivering event messages via emails, GSM short messages, onscreen event panel, or to trigger an alarm, etc. For more information, refer to the ST7501 User Manual.



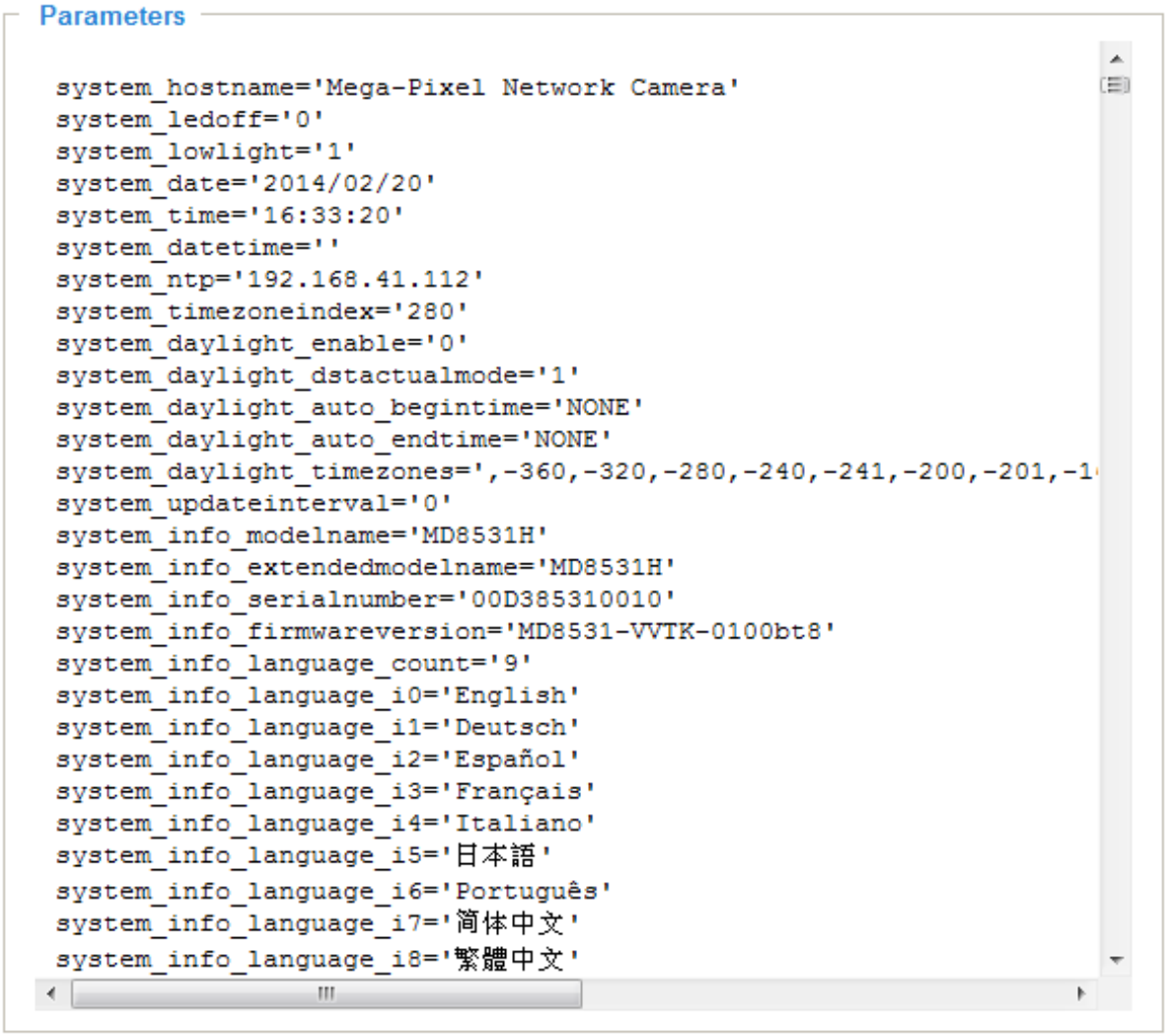
Access log



Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

System > Parameters Advanced Mode

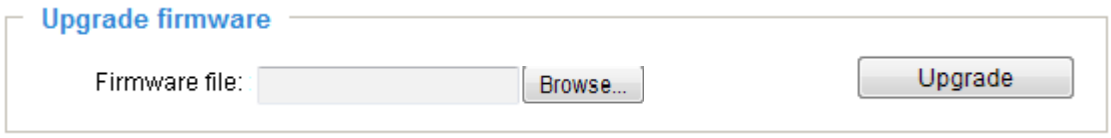
The View Parameters page lists the entire system's parameters. If you need technical assistance, please provide the information listed on this page.



System > Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

General settings > Upgrade firmware

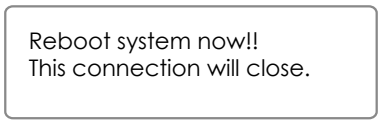


This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

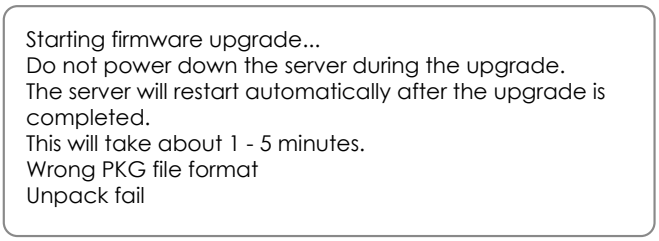
Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.

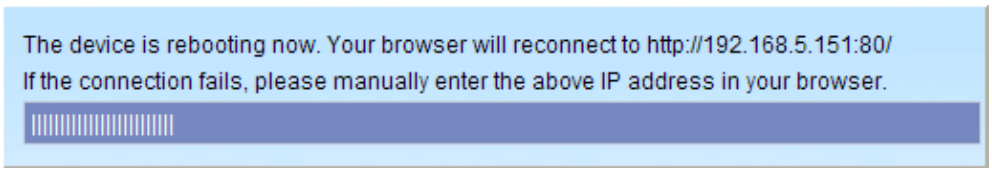


The following message is displayed when you have selected an incorrect firmware file.



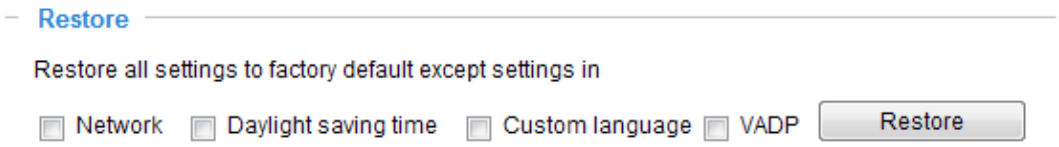
General settings > Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.



If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

General settings > Restore



This feature allows you to restore the Network Camera to factory default settings.

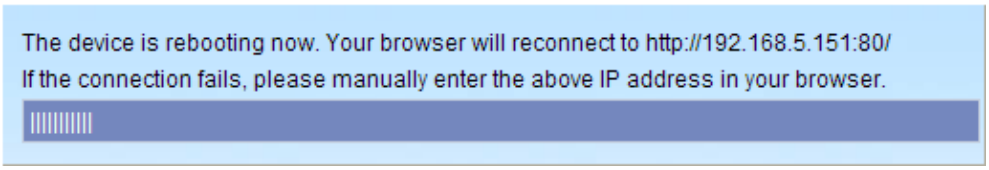
Network: Select this option to retain the Network Type settings (please refer to Network Type on page 62).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

Custom Language: Select this option to retain the Custom Language settings.

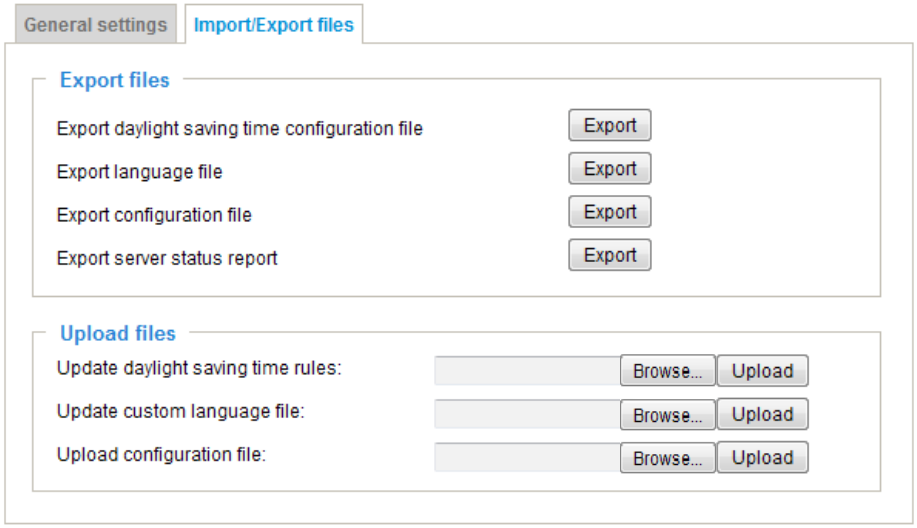
VADP: Retain the VADP modules (3rd-party software stored on the SD card) and related settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.



Import/Export files Advanced Mode

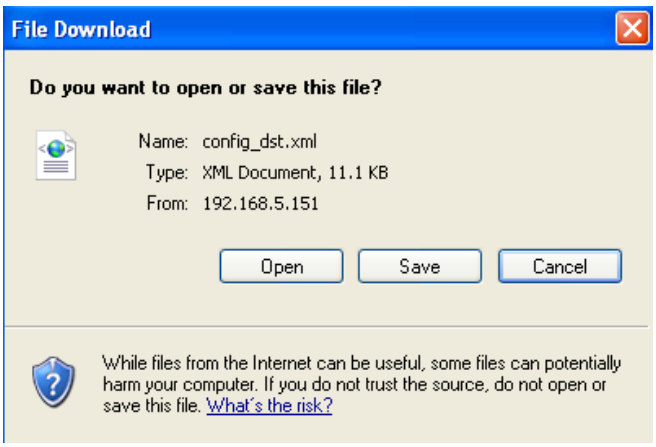
This feature allows you to Export / Update daylight saving time rules, custom language file, configuration file, and server status report.



Export daylight saving time configuration file: Click to set the start and end time of DST (Daylight Saving).

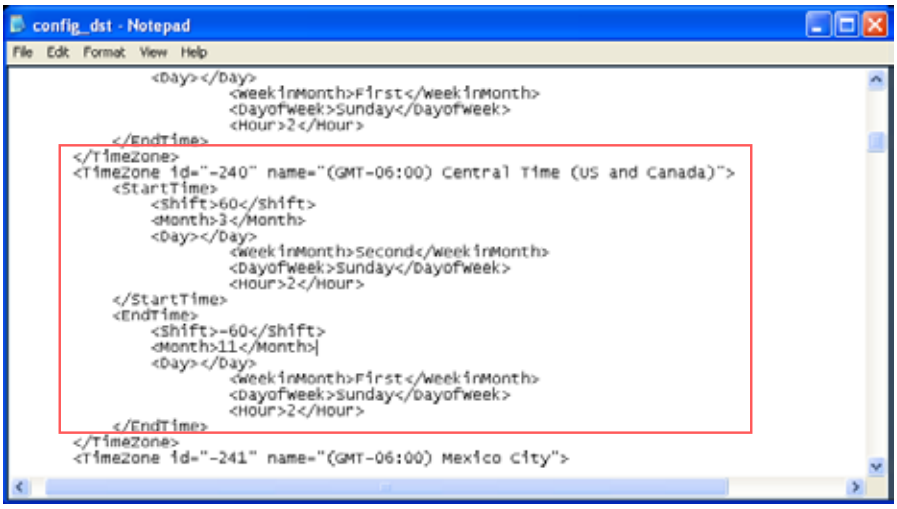
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



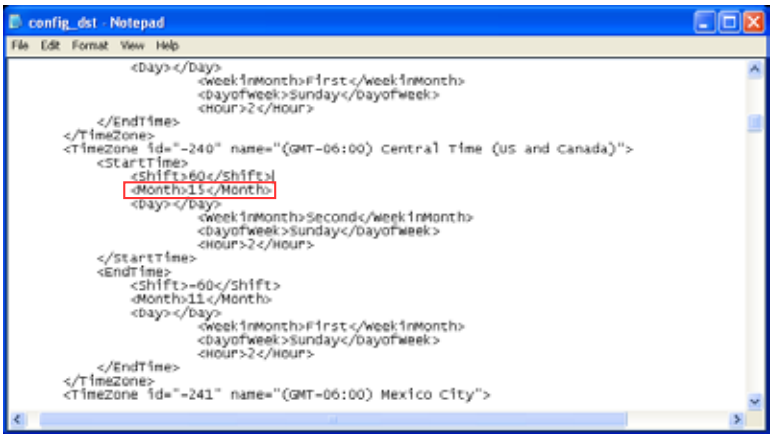
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

   In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.

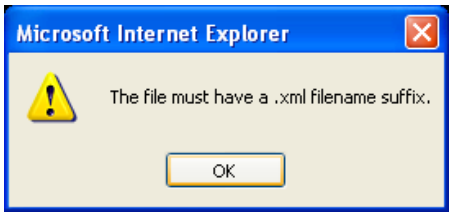


Update daylight saving time rules: Click **Browse…** and specify the XML file to update.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.



The following message is displayed when attempting to upload an incorrect file format.



Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Update custom language file: Click **Browse…** and specify your own custom language file to upload.

Export configuration file: Click to export all parameters for the device and user-defined scripts.

Update configuration file: Click **Browse…** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

Export server staus report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message ... and so on.

Tips:

- If a firmware upgrade is accidentally disrupted, say, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

  Applicable scenario:

  (1) Power disconnected during firmware upgrade.
  (2) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

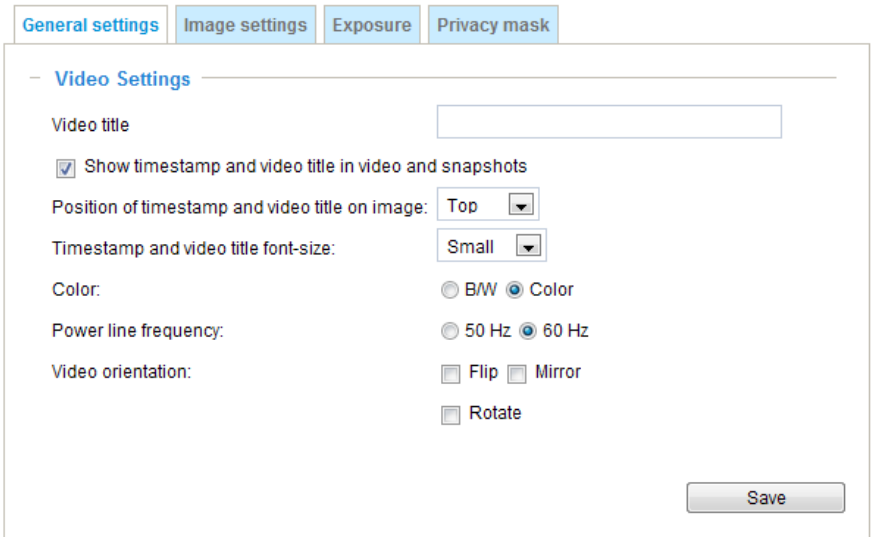
  You can use the following methods to activate the camera with its backup firmware:

  (1) Press and hold down the reset button for at least one minute.
  (2) Power on the camera until the Red LED blinks rapidly.
  (3) After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When tthis process is completed, the LED status should return to normal.

Media > Image Advanced Mode

This section explains how to configure the image settings of the Network Camera. It is composed of the following five columns: General settings, Image settings, Exposure, and Privacy mask.

General settings



Video title

Show_timestamp_and video_title_in_video_and_snapshots: Enter a name that will be displayed on the title bar of the live video as the picture shown below.

Position of timestamp and video title on image: Select to display time stamp and video title on the top or at the bottom of the video stream.

Timestamp and video title font size: Select the font size for the time stamp and title.

Color: Select to display color or black/white video streams.

Position of timestamp and video title on image: Select to display time stamp and video title on the top or at the bottom of the video stream.

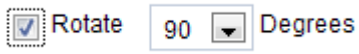
Timestamp and video title font size: Select the font size for the time stamp and title.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Video orientation:

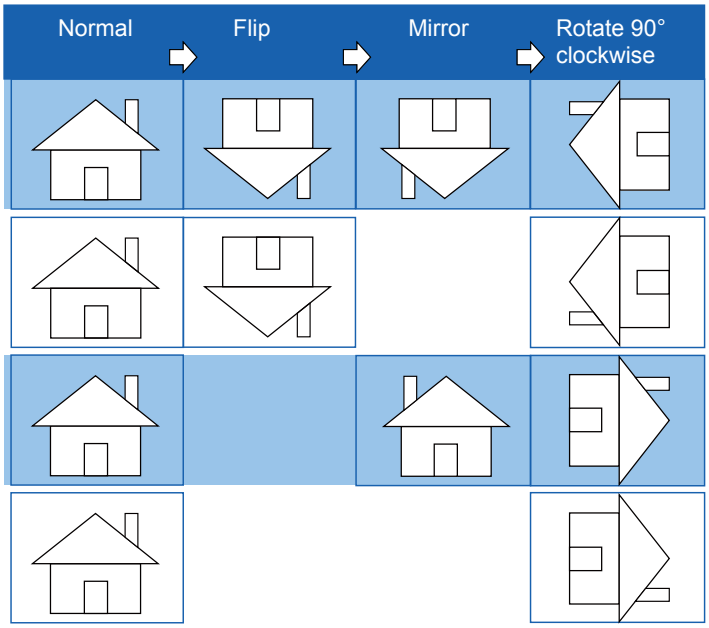
Flip - vertically reflect the display of the live video;

Mirror - horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Please note that if you have preset locations, those locations will be cleared after flip/mirror setting.

Rotate - 

The rotation here indicates clockwise rotation. Rotation can be applied with flip, mirror, and physical lens rotation (see below) settings to adapt to different mounting locations.

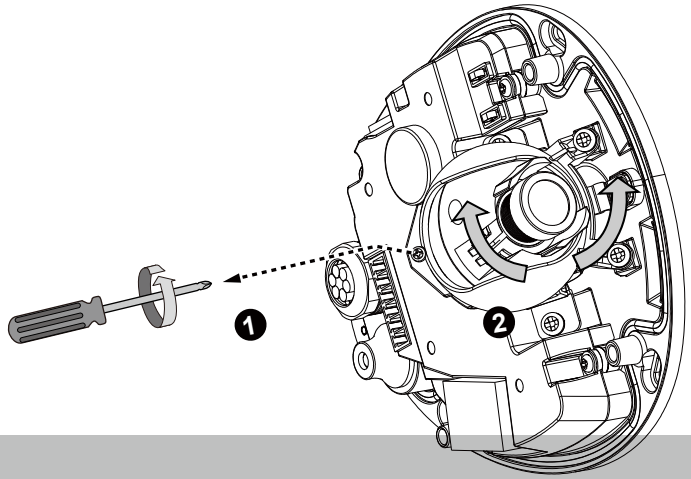
The figures in the illustration are shown in a consecutive order.



The camera may be installed on a vertical, side-facing, or tilted surface in order to accommodate the interior or exterior design of a vehicle. Because the interior of a transportation vehicle is often shaped as a narrow rectangular space, the conventional HD image, such as that of a 16:9 aspect ratio, will be incongruous with its wide horizontal view. With video rotation, the camera can more readily cover the field of view on a vehicle.

In addition to video rotation, if the camera is mounted on a tilted surface, you can:

1. Loosen the retention screw.
2. Rotate the lens module to adapt to the mount position. When done, fasten the retention screw.



Below is an example showing a camera mounted on a side panel tilted 30° from a vertical wall. You can rotate the camera video to 270° and manually rotate the lens module slightly counter-clockwise. The result will be a narrow, tall, rectangle view.

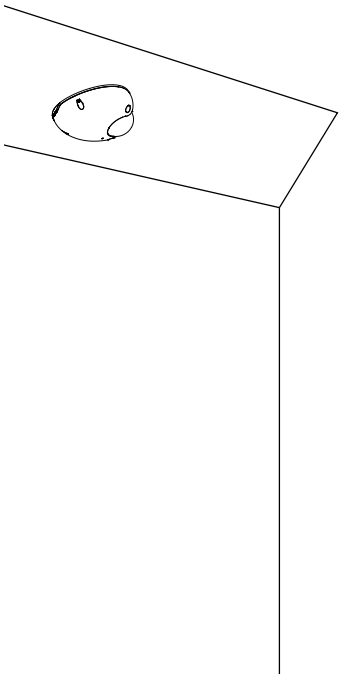
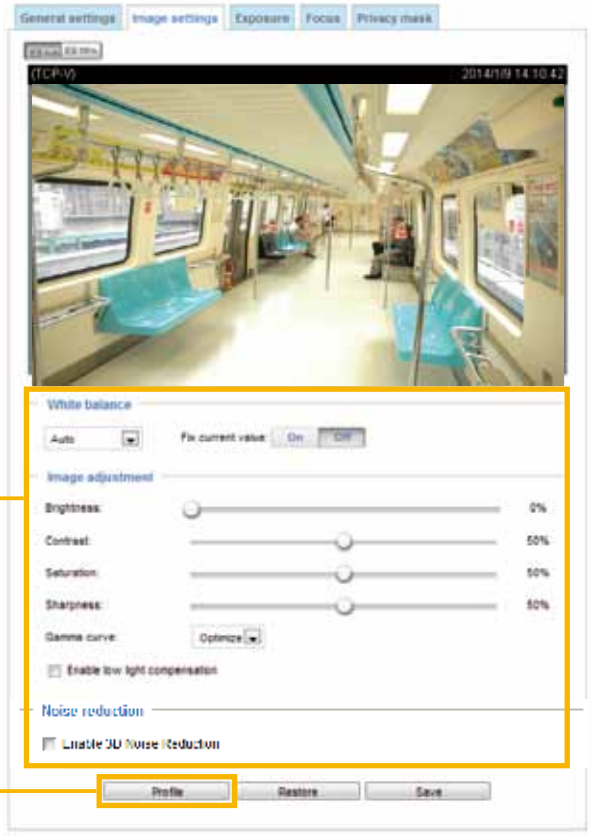


Image settings

On this page, you can tune the White balance and Image adjustment.



White balance: Adjust the value for the best color temperature.

■ You may follow the steps below to adjust the white balance to the best color temperature.

1. Place a sheet of paper of white or cooler-color temperature color, such as blue, in front of the lens, then allow the Network Camera to automatically adjust the color temperature.
2. Click the **On** button to **Fix current value** and confirm the setting while the white balance is being measured.

■ Using the **Manual mode**, you may also manually tune the color temperature by pulling the RGain and BGain slide bars.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from 0% to 100%.

■ Contrast: Adjust the image contrast level, which ranges from 0% to 100%.

■ Saturation: Adjust the image saturation level, which ranges from 0% to 100%.

■ Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.

■ Gamma curve: Adjust the image sharpness level, which ranges from 0 to 0.45.
You may let firmware Optimize your display or select a value to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.

■ Enable low light compensation: Select this option in low light mode, and the values of sharpness and brightness will change automatically. This function also benefits from an automated noise reduction feature.

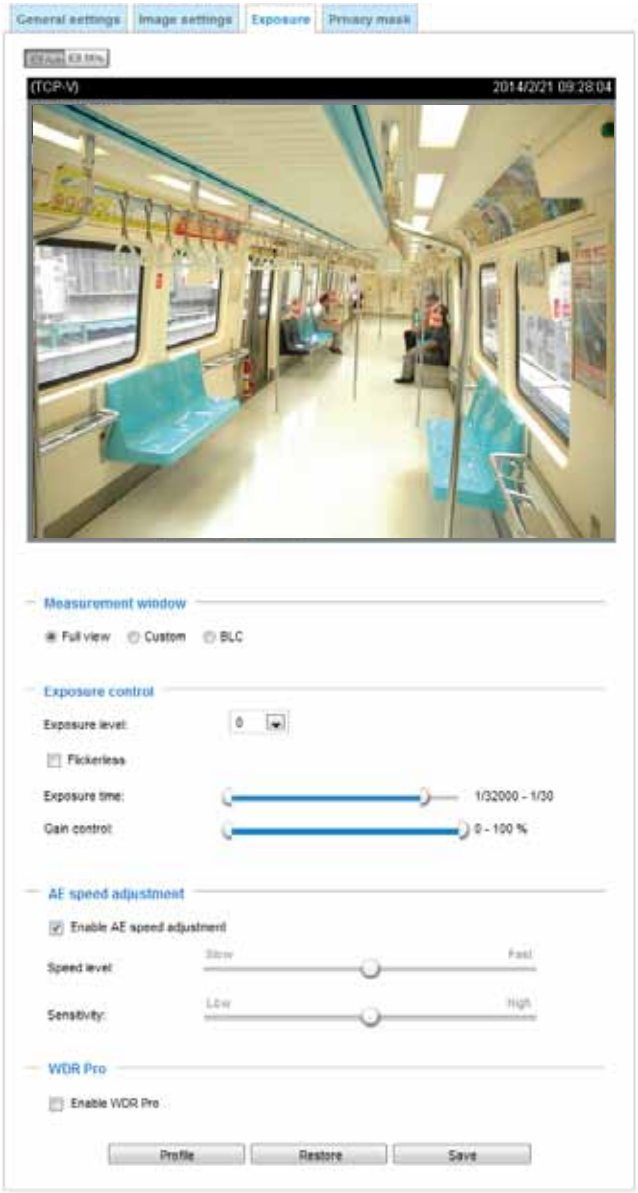
Noise reduction

■ Enable 3D noise reduction: Check to enable noise reduction in order to reduce noises and flickers in image. This applies to the onboard 3D Noise Reduction feature. Use the pull-down menu to adjust the reduction strength. Note that applying this function to the video channel will consume system computing power.

3D Noise Reduction is mostly applied in low-light conditions. When enabled in a low-light condition with fast moving objects, trails of after-images may occur. You may then select a lower strength level or disable the function.

Exposure Advanced Mode

On this page, you can set the Measurement window, Exposure control, AE speed, and WDR Pro. Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.



Measurement Window: This function allows user to set measurement window(s) for low light compensation.

■ Full view: Calculate the full range of view and offer appropriate light compensation.

■ Custom: This option allows you to manually add a specific window as a measuring area. The measuring window refers to “weighed window“ where the lighting condition within the particular area is taken into account. The Exclude window tells the firmware to ignore the lighting condition of a specific area. Camera firmware then adopts the weighted averages method to calculate the value. You can create up to 10 inclusive and exclusive windows.

■ BLC: When selected, a BLC window will appear on screen meaning that the center of the scene will be taken as a weighed area. This option enables light compensation for images that are too dark or too bright to recognize; for example, for the dark side of objects that is posed against bright sunlight.

Exposure control:

■ **Exposure level**: You can manually configure the Exposure level, which ranges from -2.0 to +2.0 (dark to bright). You can click and drag the pointers on the **Exposure time** and **Gain control** slide bars to specify a range of shutter time and Gain control values within which the camera can automatically tune to an optimal imaging result. You may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.

■ **Flickerless**: This function helps avoid the flickering on images because of the fast shutter movement. When selected, the exposure time will be forced to stay longer than 1/120 second.

■ **Exposure Time**: The configurable max. exposure time is tunable according to lighting conditions with values ranging from 1/32000 to 1/5 of a second.

■ **Gain Control**: Tune the slider bar to set the Gain Control to the best image quality. Higher gain control value will generate a certain amount of noises.

■ **AE speed adjustement**: AE (Automatic Exposure)

AE automatically controls iris opening size for the varying levels of brightness. The conversion speed, if this function is enabled, is configurable for varying lighting conditions. This makes the camera well-adapted to fast changes in lighting conditions, such as entering or leaving a tunnel. The Sensitivity option determines how fast the AE speed adjustment adapts to the changes in the environment.

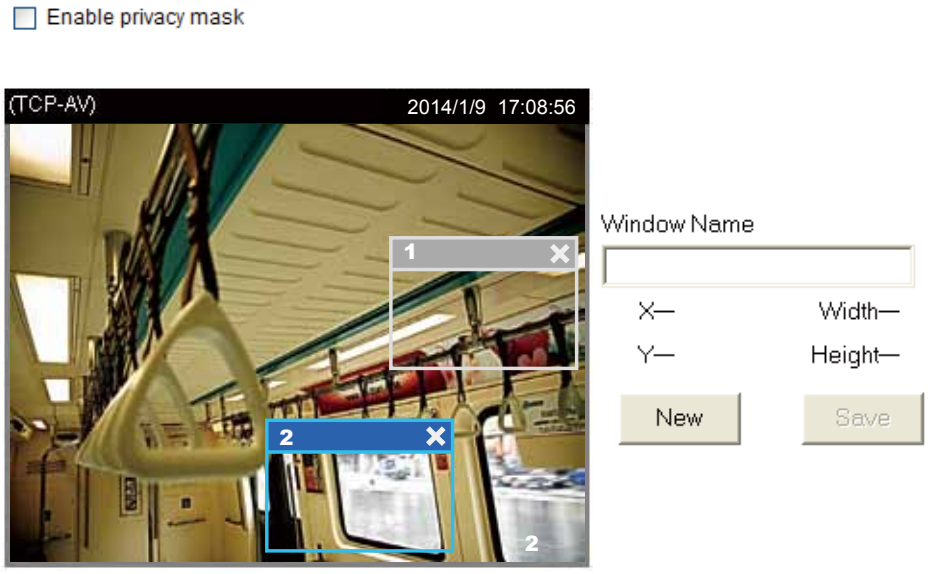
■ **WDR Pro** : When enabled, you can select the strength of the WDR function. The Low, Medium, High options correspond to the level of contrast between the overly-lit area and the shaded areas. For example, the High option applies to a high contrast scenario. Note that when the exposure time is set to longer than 1/60 second, the WDR function will be disabled.

The Sensitivity option applies to the response speed to the change in bright-to-dark lighting contrast.

You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings.

Privacy mask Advanced Mode

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.



■ To set the privacy mask windows, follow the steps below:

1. Click **New** to add a new window.
2. You can use the mouse cursor to size and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Click on the **Enable privacy mask** checkbox to enable this function.

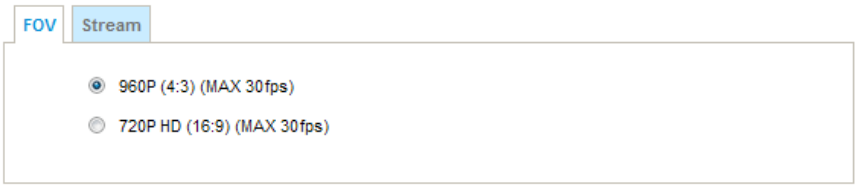
NOTE:

► *Up to 5 privacy mask windows can be set up on the same screen.*

► *If you want to delete the privacy mask window, please click the 'x' on the upper right corner of the window.*

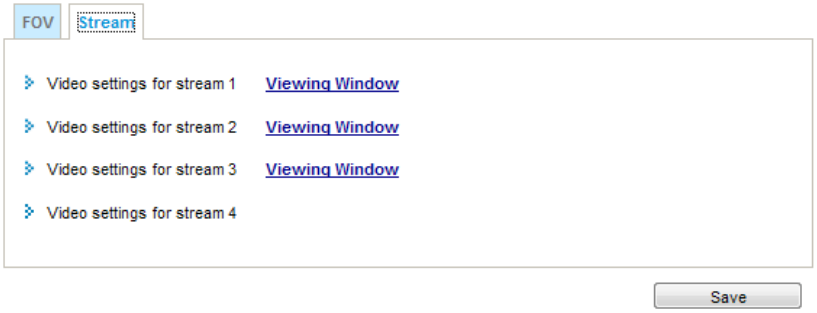
Media > Video Advanced Mode

FOV



You might select different resolutions, 960P and 720P, with different aspect ratios, 4:3 or 16:9 for the video streams. Note that changing the FOV will erase your preset points, Motion detection, exposure window, and privacy masks settings.

Stream settings



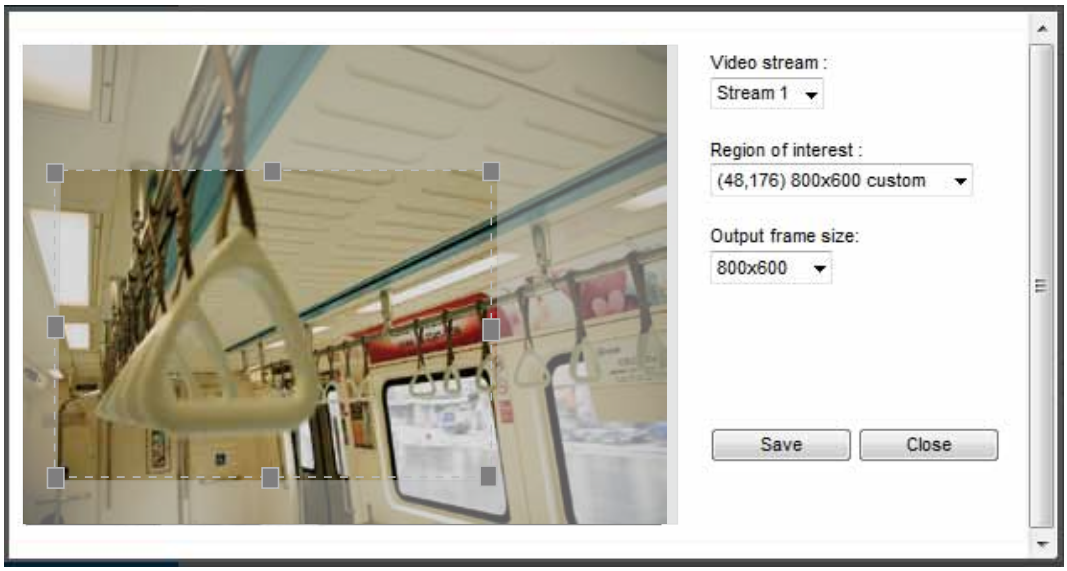
This Network Camera supports multiple streams with frame sizes ranging from 176 x 144 to 1280 x 960.

The definition of multiple streams: (the following is based on the selection of 960P FOV)

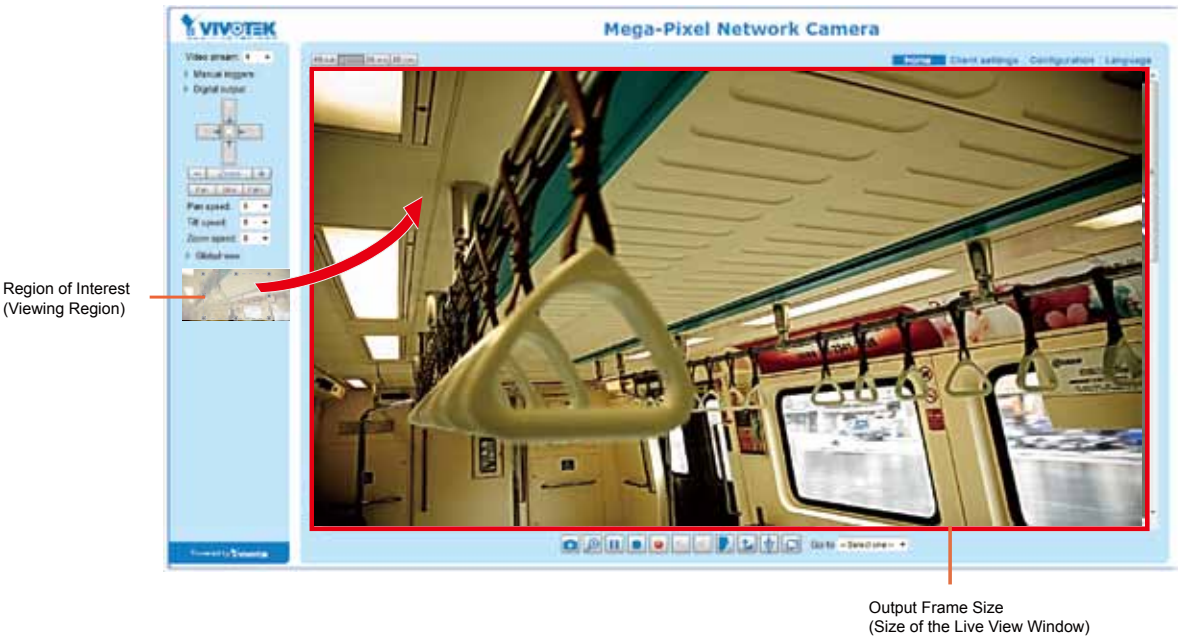
- Stream 1: The default frame size for Stream 1 is set to the 1280 x 960 at 30fps.
- Stream 2: The default frame size for Stream 2 is set to the 800 x 600 at 30fps.
- Stream 3: The default frame size for Stream 3 is set to the 640 x 480 at 15fps.
- Stream 4: The default frame size for Stream 4 is set to the 1280 x 960 at 30fps.

Please follow the steps below to set up those settings for a viewing window:

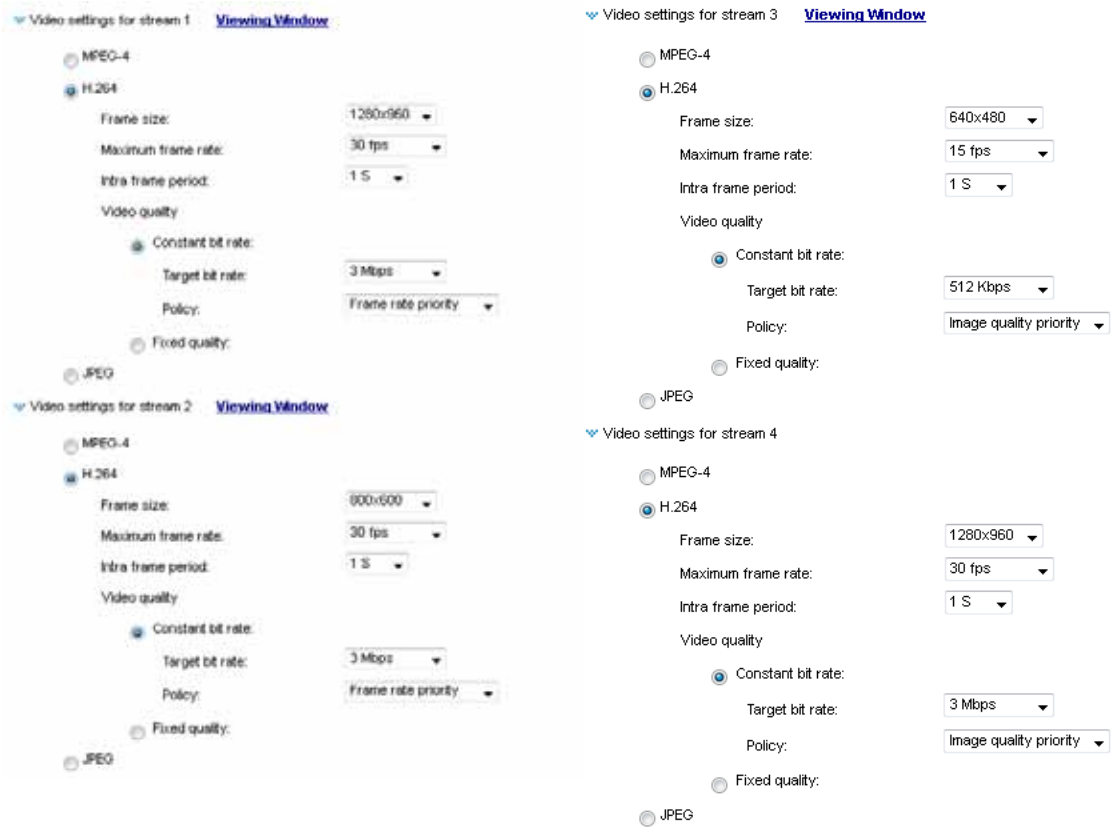
1. Select a stream for which you want to set up the viewing region.
2. Select a **Region of Interest** from the drop-down list. The floating frame, the same as the one in the Gloabl View window on the home page, will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.
3. Choose a proper **Output Frame Size** from the drop-down list according to the screen size of your monitoring device.



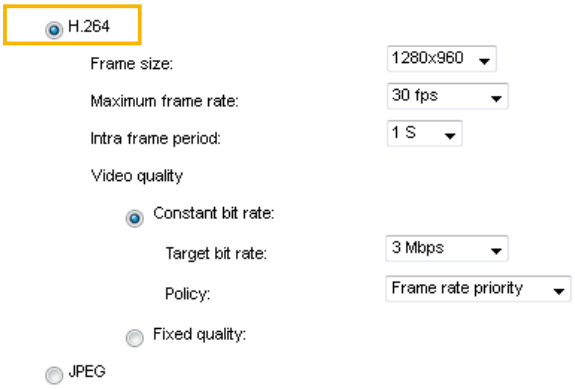
Click **Viewing Window** to open the viewing region settings page. On this page, you can configure the Region of Interest and the Output Frame Size for different streams. For example, you can crop only a portion of the image that is of your interest, and thus save the bandwidth needed to transmit the video stream. As the picture shown below, the area of your interest in a parking lot should the vehicles. The blue sky is of little value for the surveillance purpose.


Region of Interest
(Viewing Region)
Mega-Pixel Network Camera
Output Frame Size
(Size of the Live View Window)

Click the stream item to display the detailed information. The maximum frame size will follow your settings in the above Viewing Window sections.



This Network Camera provides real-time H.264, MPEG-4, and MJPEG compression standards (Triple Codec) for real-time viewing. If the **H.264** mode is selected, the video is streamed via RTSP protocol. There are several parameters through which you can adjust the video performance:



■ Frame size

You can set up different video resolutions for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more network bandwidth.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps.

■ Intra frame period

Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality

- **Constant bit rate**: A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, and 8Mbps. You can also select **Customize** and manually enter a value.

  - **Target bit rate**: select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 16Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The Network Camera will strive to deliver video streams around or within the bit rate limitation you impose.

  - **Policy**: If **Frame Rate Priority** is selected, the Network Camera will try to maintain the frame rate per second performance, while the image quality will be compromised. If **Image quality priority** is selected, the Network Camera may drop some video frames in order to maintain image quality.

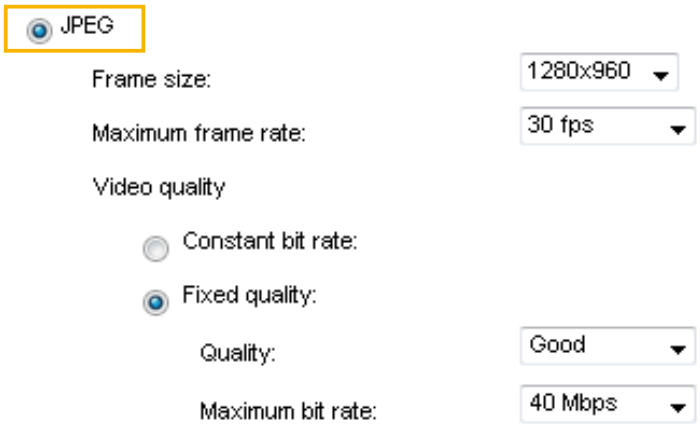
- **Fixed quality:** On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

  - **Maximum bit rate**: With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 40Mbps.

  The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gain.

  You may also manually enter a bit rate number by selecting the **Customized** option.

If **JPEG** mode is selected, the Network Camera sends consecutive JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:



■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. The frame rate will decrease if you select a higher resolution.

■ Video quality
Refer to the previous page setting an average or upper bound threshold for controlling the bandwidth consumed for transmitting motion jpegs. The configuration method is identical to that for MPEG4 and H.264.

For Constant Bit Rate and other settings, refer to the previous page for details.

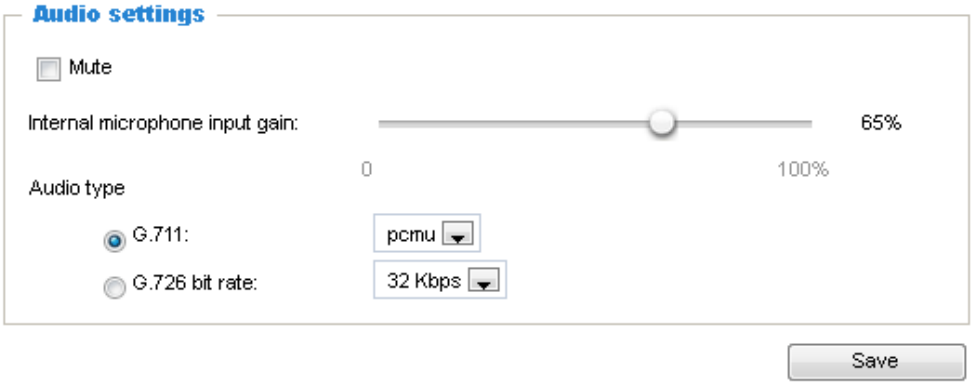
NOTE:

► *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

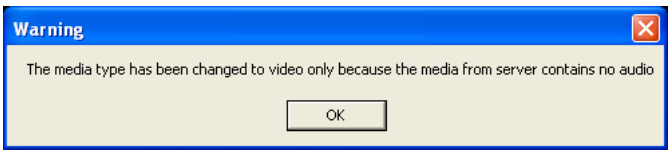
► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Media > Audio

Audio Settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if muted, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:



Internal microphone input gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from 21dB (most sensitive) to -33 dB (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.

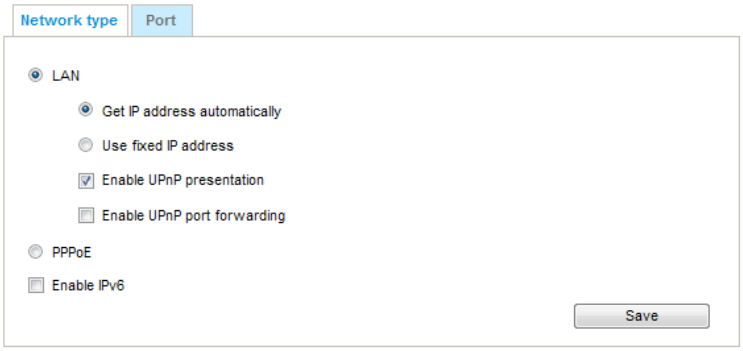
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.
- G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

When completed with the settings on this page, click **Save** to enable the settings.

Network > General settings

This section explains how to configure a wired network connection for the Network Camera.

Network Type

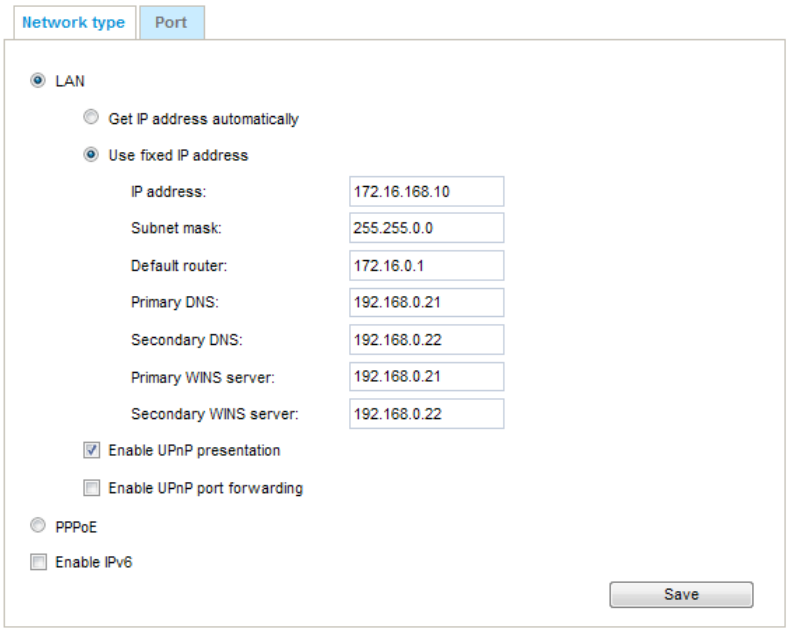


LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Please rememer to click on the **Save** button when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.



1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 16 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.

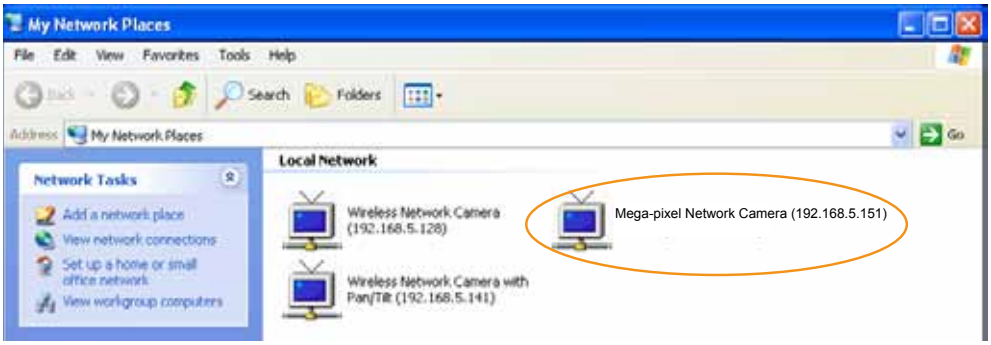
Primary DNS: The primary domain name server that translates host names into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer names and IP addresses.

Secondary WINS server: The secondary WINS server that maintains the database of computer names and IP addresses.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, the shortcuts to connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



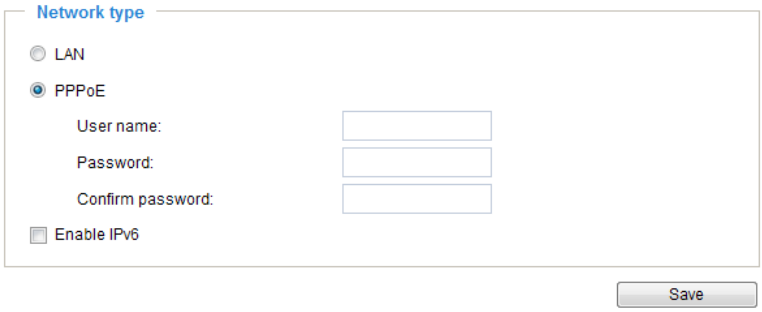
Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports automatically on the router so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 101) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 106).
   Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

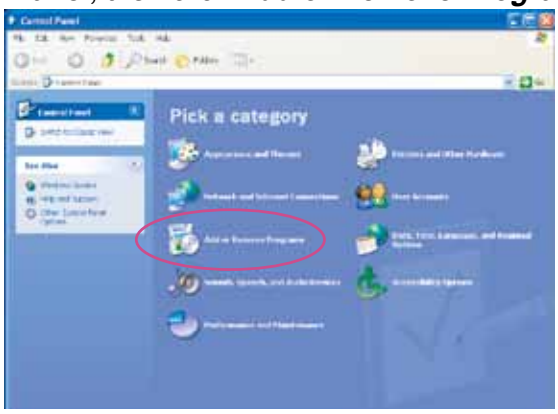
NOTE:

► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

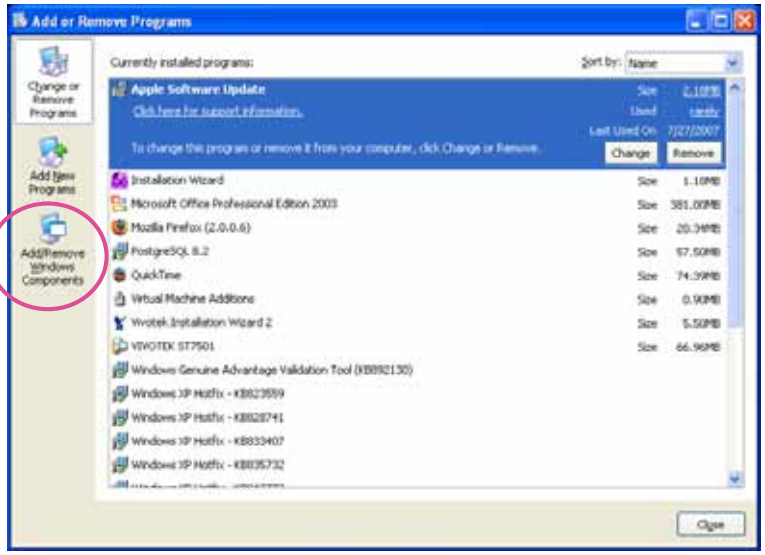
► *If UPnP™ is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable the UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

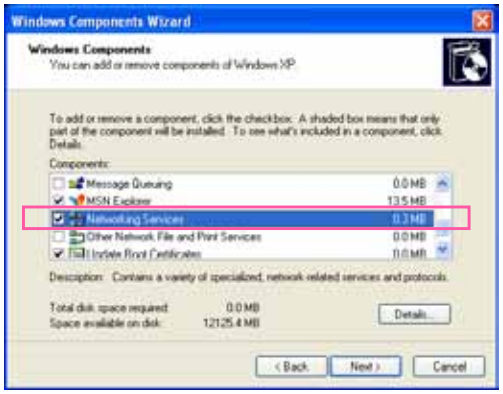
1. *Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



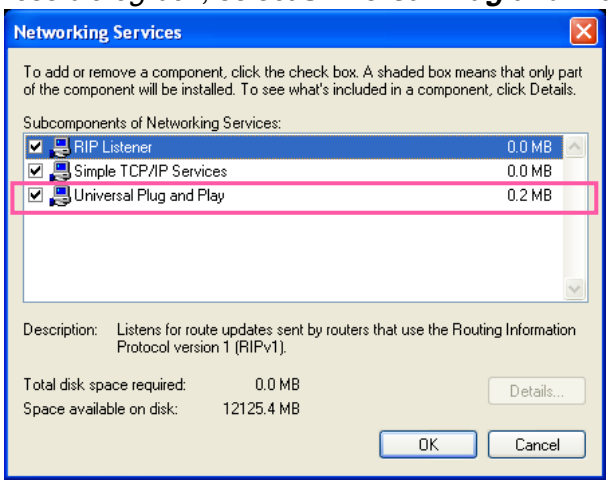
2. *In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



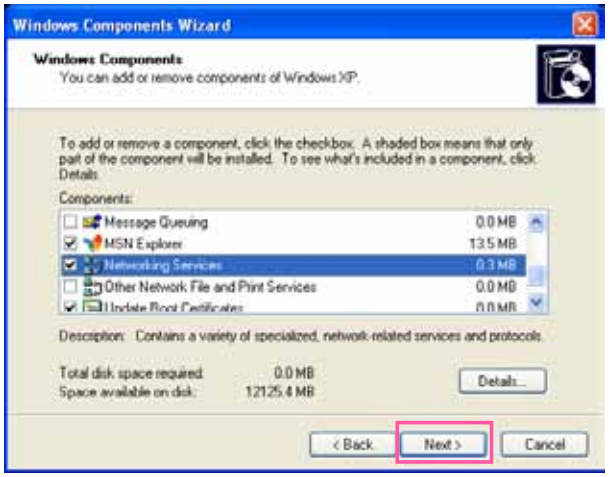
3. *In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*



4. In the Networking Services dialog box, select ***Universal Plug and Play*** and click ***OK***.



5. Click ***Next*** in the following window.



6. Click ***Finish***. *UPnP™ is enabled.*

► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

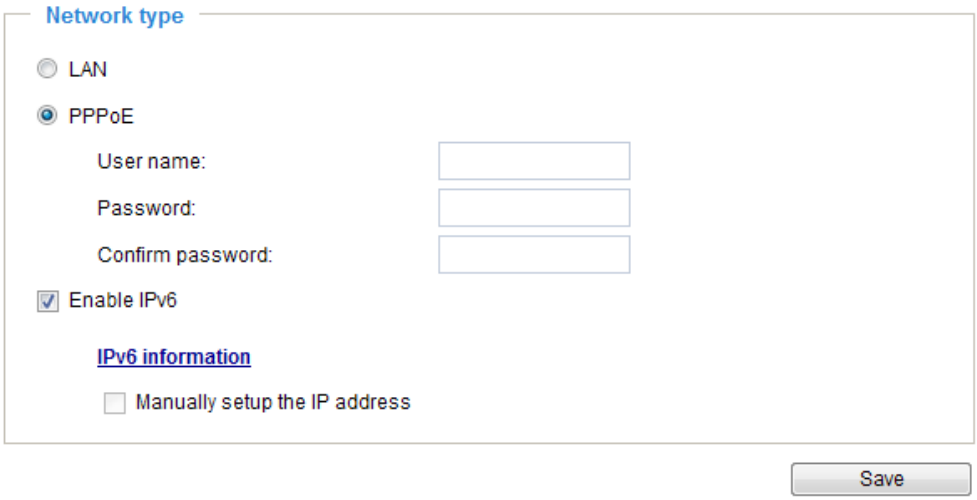
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 45 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

Enable IPv6

Select the Enable IPv6 checkbox and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 7 or 8, Mozilla Firefox 13.0 or above.

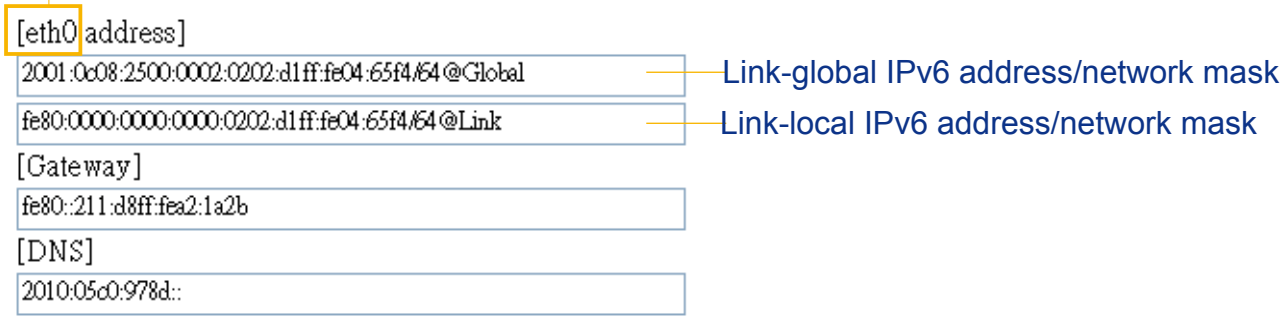


When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

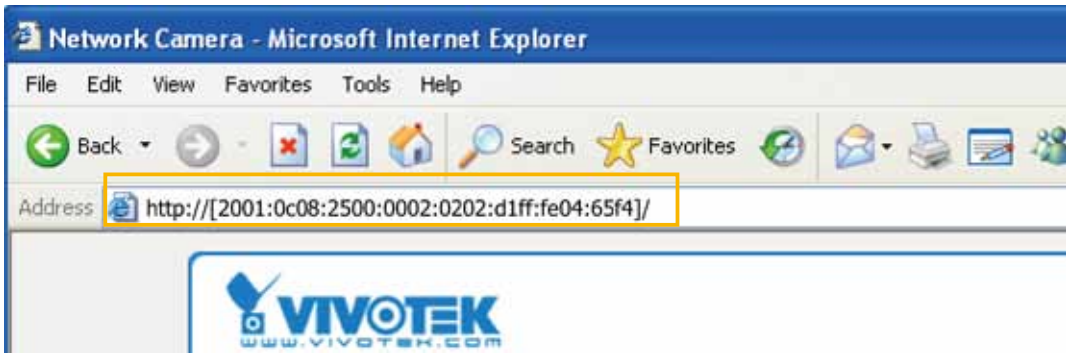
If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:

Refers to Ethernet



Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

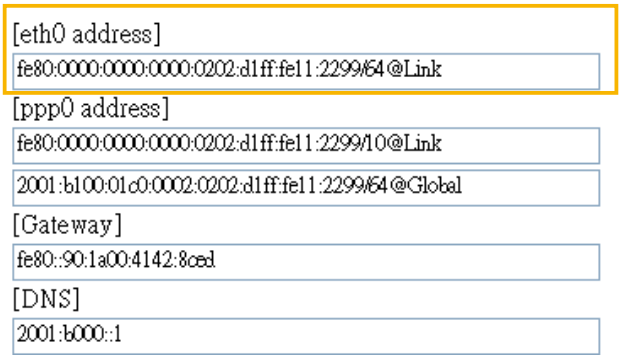
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:



NOTE:

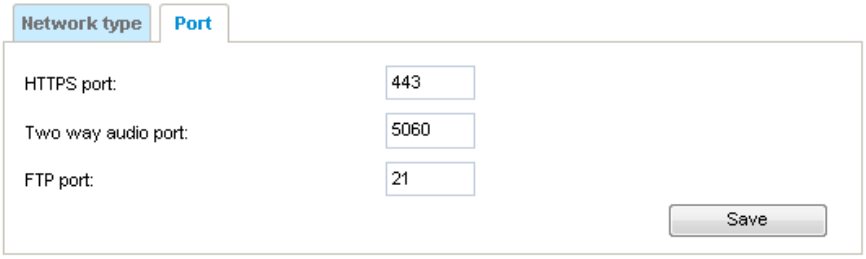
► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage using the following address format: (Please refer to **HTTP** streaming on page 69 for detailed information.)*

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*



Manually setup the IP address: Select this option to manually configure IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers. If you check this item, the following blanks will be displayed for you to enter the corresponding information:

Port

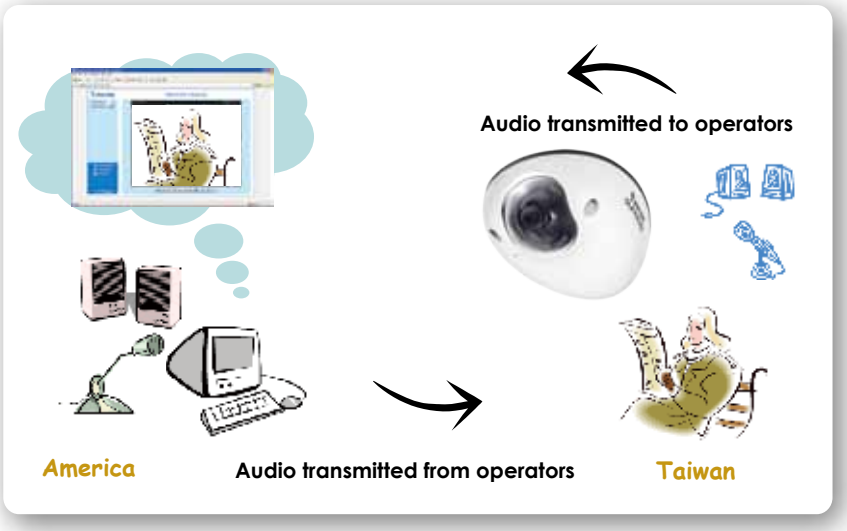


HTTPS port: By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio port: By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" or "H.264" on the Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 31 and Stream settings on page 56.

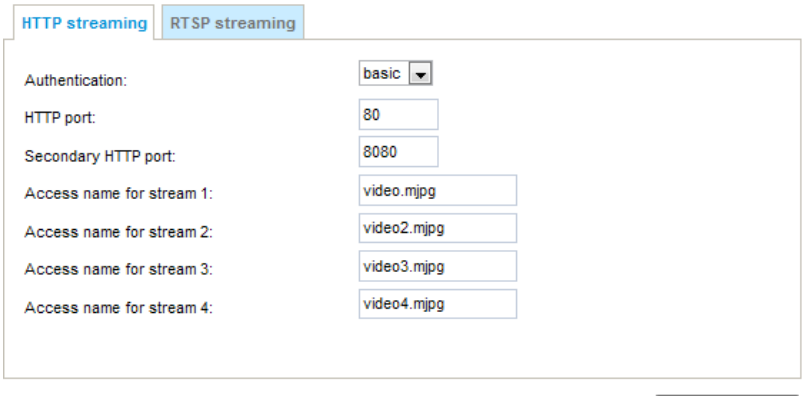


FTP port: The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

Network > Streaming protocols Advanced Mode

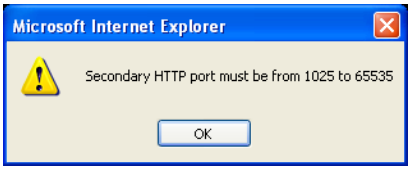
HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 79 for details.



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

On the LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for individual streams: This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 55.

When using **Mozilla Firefox** to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox.

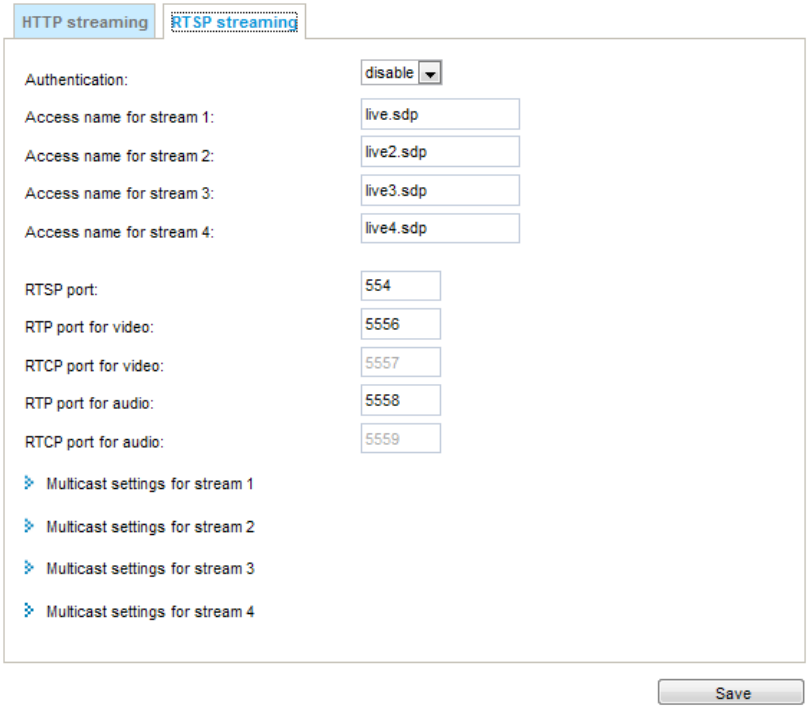
URL command -- http://<ip address>:<http port>/<access name for stream 1~4>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.

NOTE:

► *Microsoft® Internet Explorer does not support server push technology; therefore, you will not be able to access a video stream using http://<ip address>:<http port>/<access name for stream 1~4> .*

RTSP Streaming

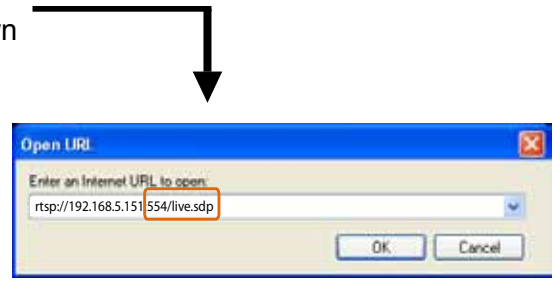
To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. Please refer to Security > User account on page 79 for details.



Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed below:

	Quick Time player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

Access name for video streams: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you have to set the video mode to H.264 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 5>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.

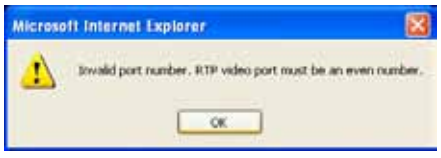


RTSP port /RTP port for video and RTCP port for video

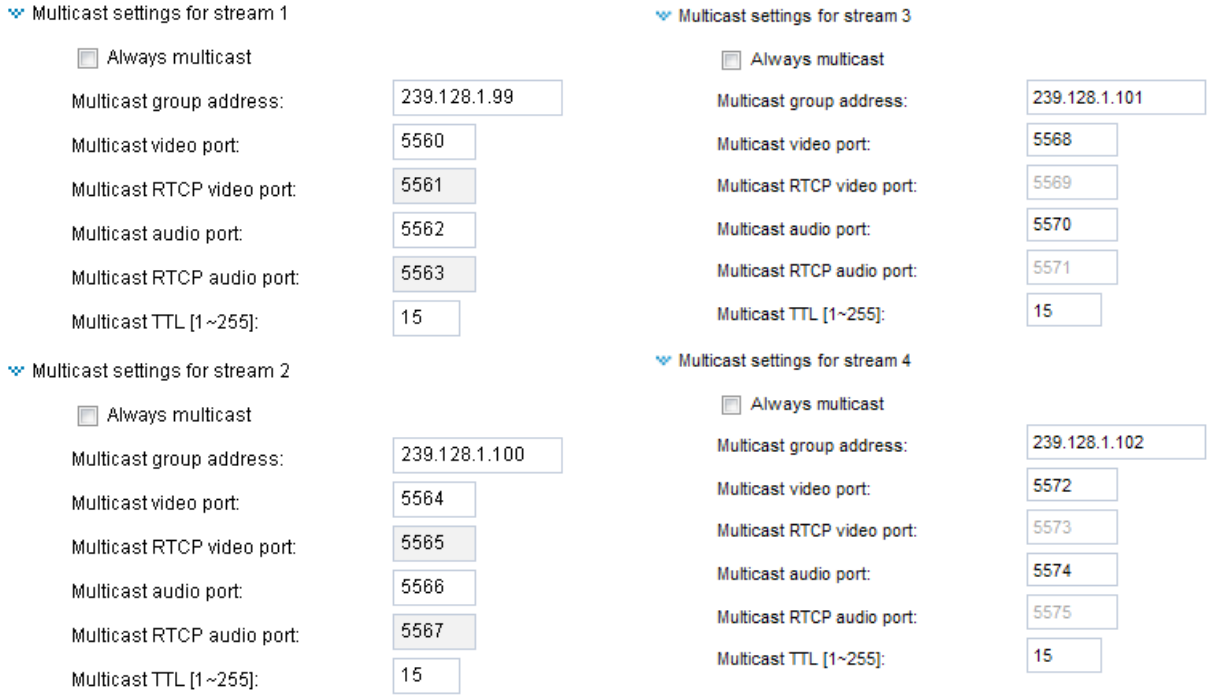
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video data to the clients. By default, the RTP port for video is set to 5556.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:



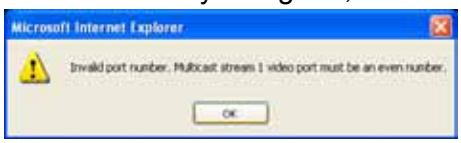
Multicast settings for stream #: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for different video streams.



Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:



Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

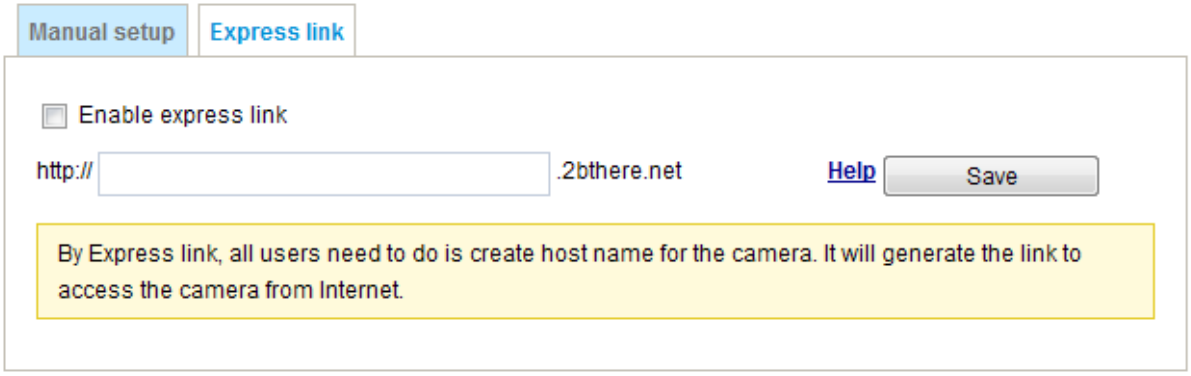
Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

Network > DDNS

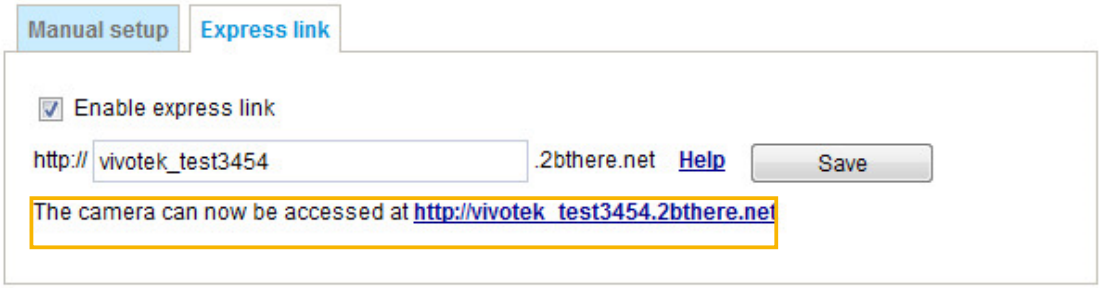
This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

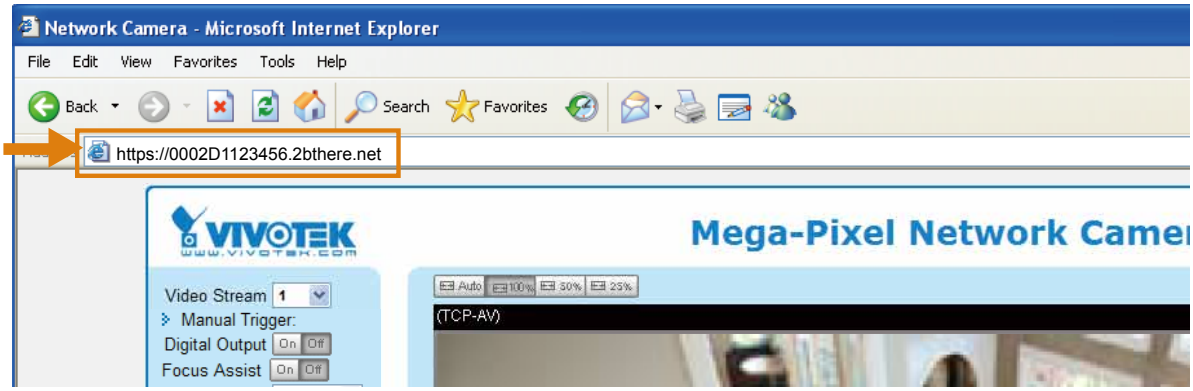
Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will examine if the host name is valid and automatically open a port on your router. If using DDNS, the user has to manually configure UPnP port forwarding. Express Link is more convenient and easier to set up.



Please follow the steps below to enable Express Link:
1. Make sure that your router supports UPnP port forwarding and it is activated.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will display a message as shown below.





Manual setup

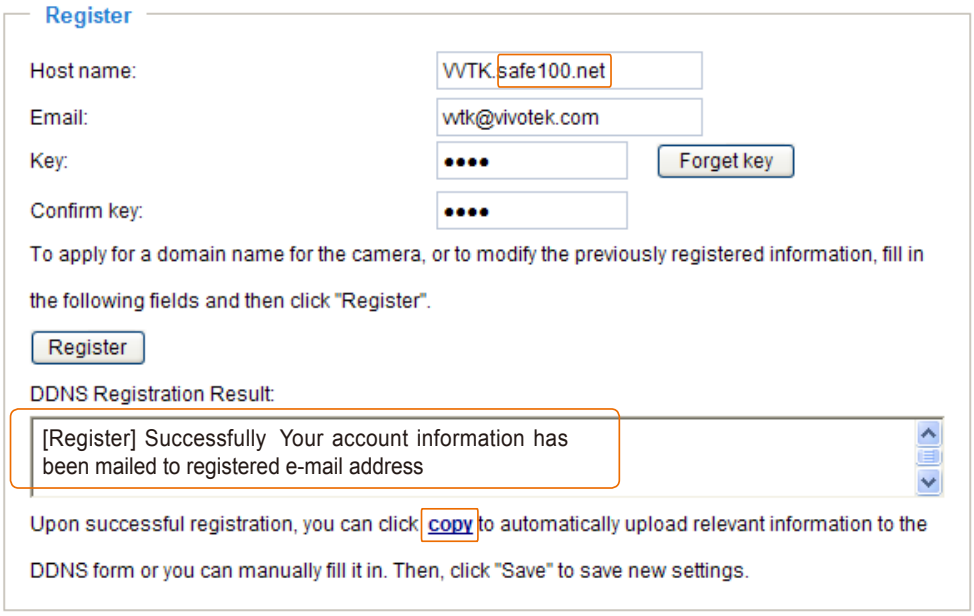
DDNS: Dynamic domain name service

Enable DDNS: Select this option to enable the DDNS setting.

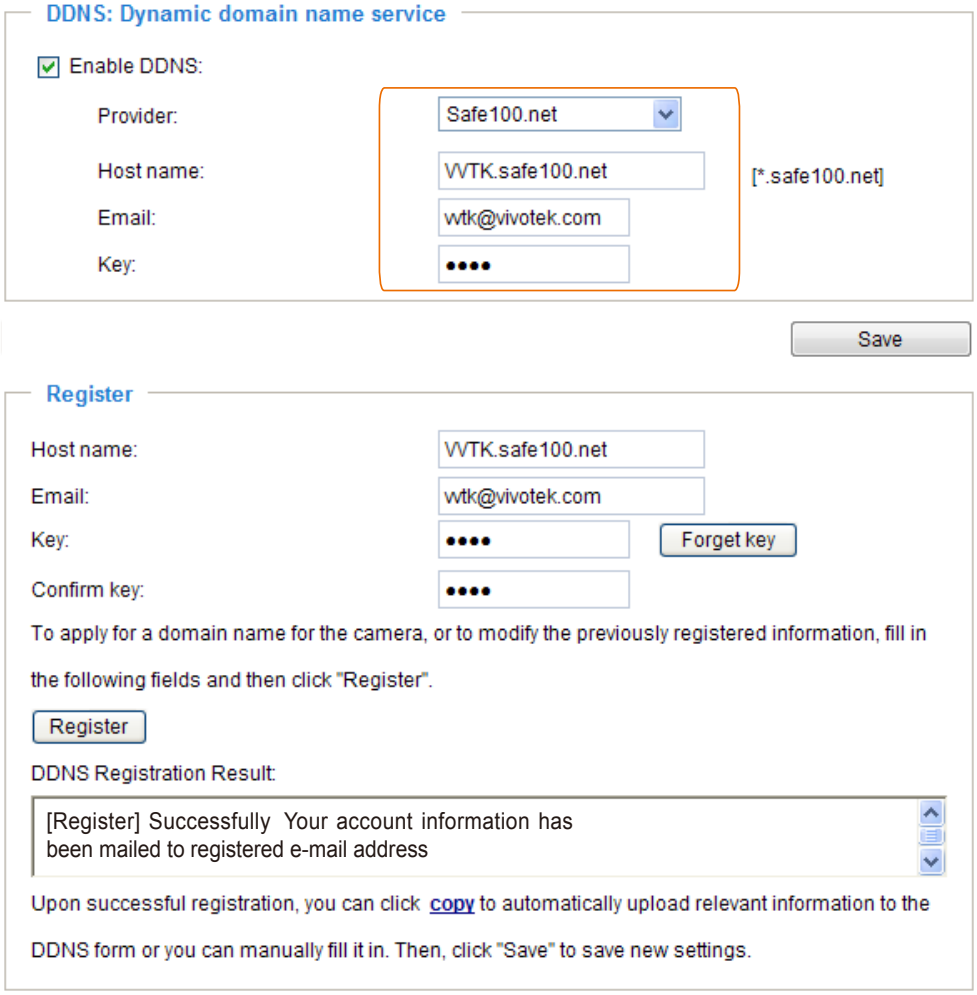
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), CustomSafe100, and dyn-interfree.it. Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.



3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.



4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Server name, Email, Key, and Confirm Key; then click **Register**.

   Enter “ns1.safe100.net” as the Server name.

   After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/

Network > QoS (Quality of Service) Advanced Mode

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:
- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).

If you assign Video the highest level, the switch will handle video packets first.

NOTE:

► *A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.*

► *The Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

Network > SNMP (Simple Network Management Protocol)

Advanced Mode

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c

Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

Enable SNMPv3

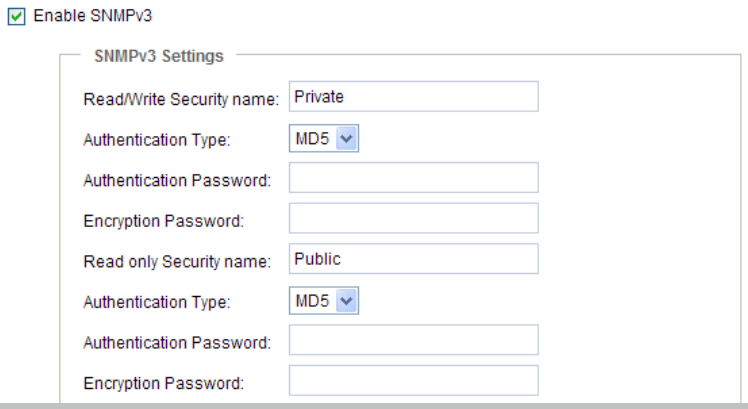
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authentication (at least 8 characters).

■ Encryption password: Enter a password for encryption (at least 8 characters).



Security > User Account

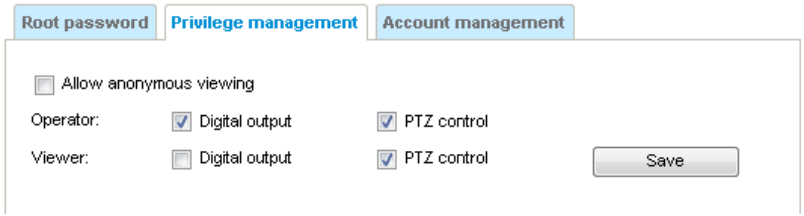
This section explains how to enable password protection and create multiple accounts.

Root Password

The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

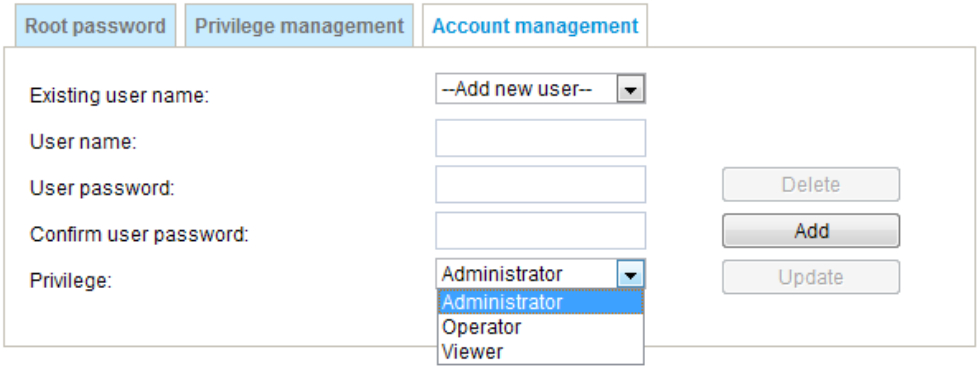
Privilege Management Advanced Mode



Digital Output & PTZ control: You can modify the manage privilege of operators or viewers. Select or deselect the checkboxes, and then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 35).

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password.

Account management



Administrators can add up to 20 user accounts.
1. Input the new user's name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer):

Administrator - Only administrators can access the Configuration page.
Operator - Although operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 129.
Viewer - Viewers access only the main page for live viewing.

Here you also can change a user's access rights or delete user accounts.
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

Security > HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

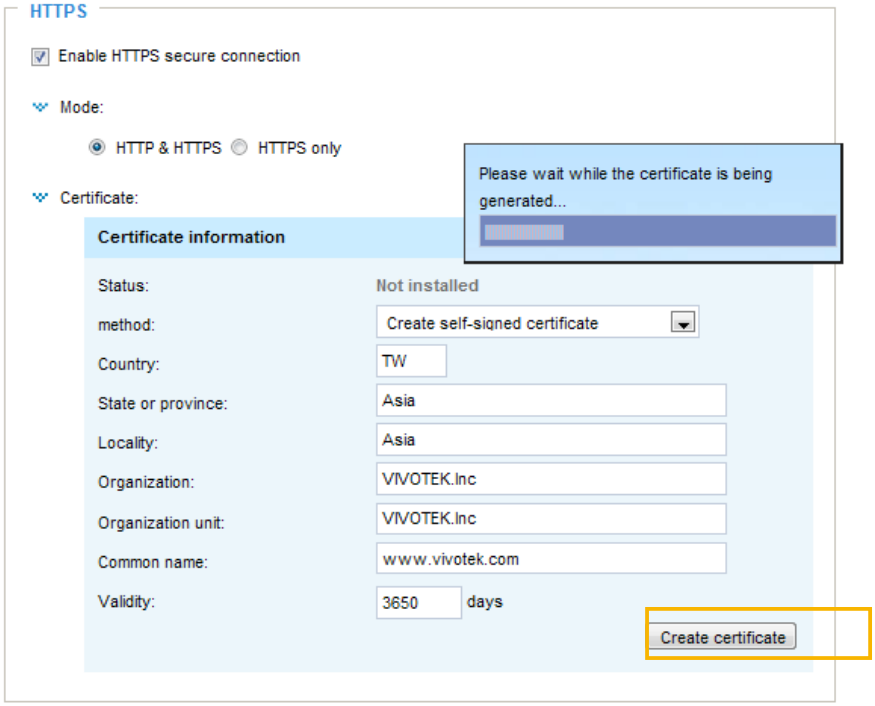
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

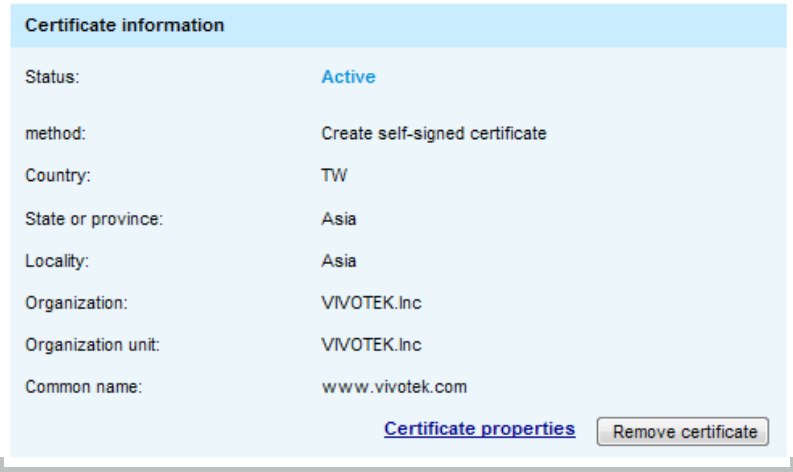
Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate

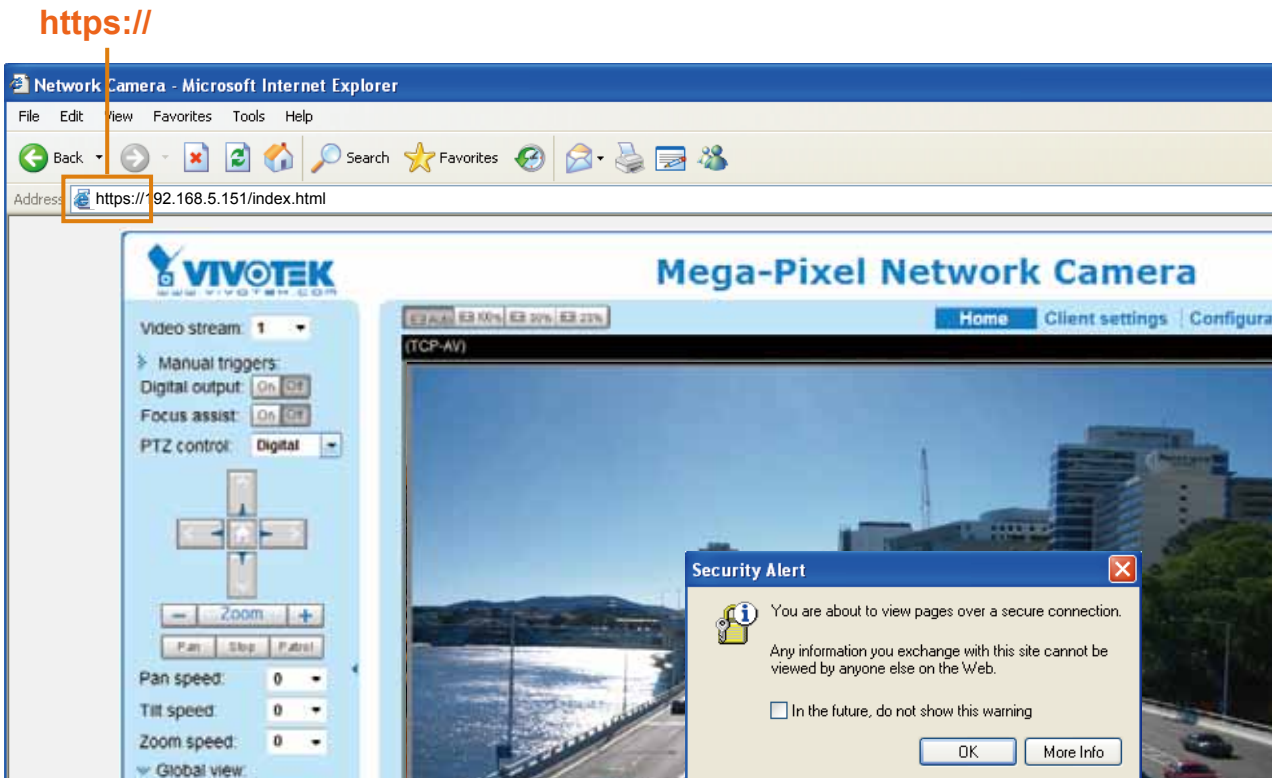
1. Select this option from a pull-down menu.
2. In the first column, select **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Create certificate** to generate a certificate.

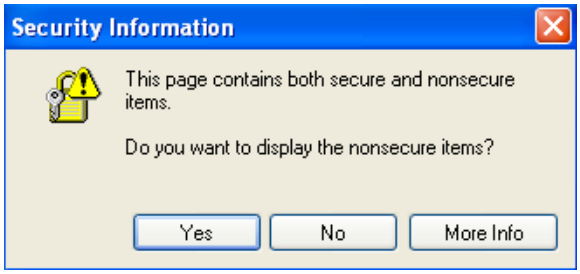


4. The Certificate Information will automatically be displayed as shown below. You can click **Certificate properties** to view detailed information about the certificate.



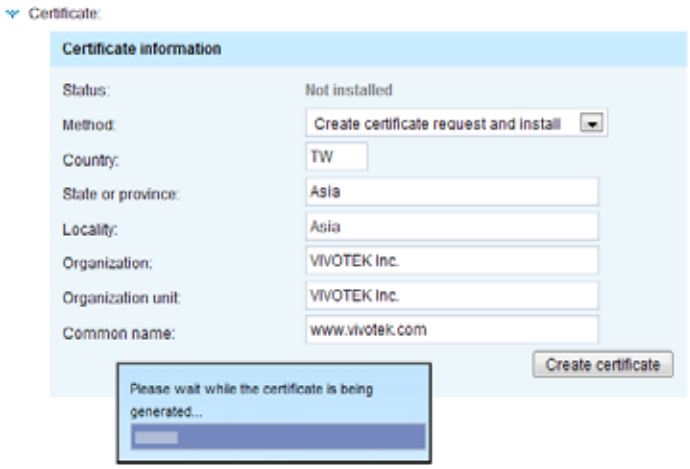
5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



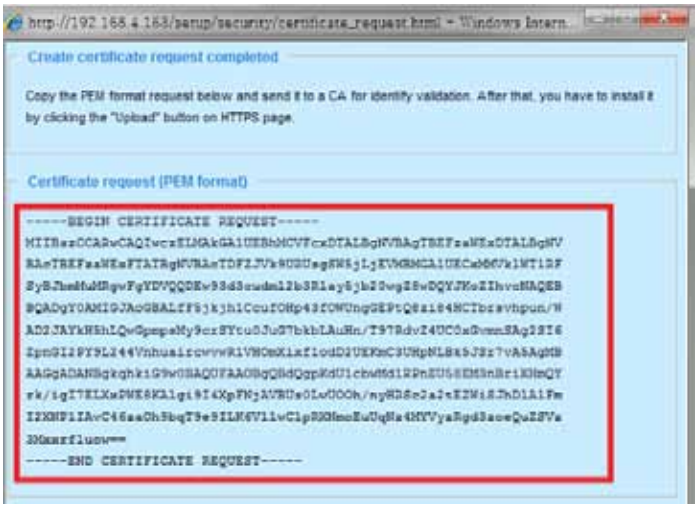


Create certificate request and install

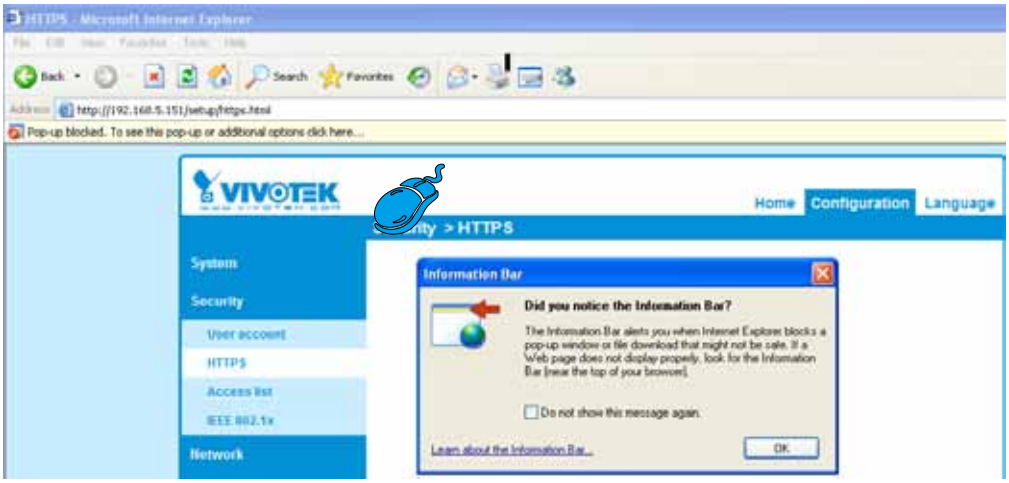
1. Select the option from the **Method** pull-down menu.
2. Click **Create certificate** to proceed.
3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.



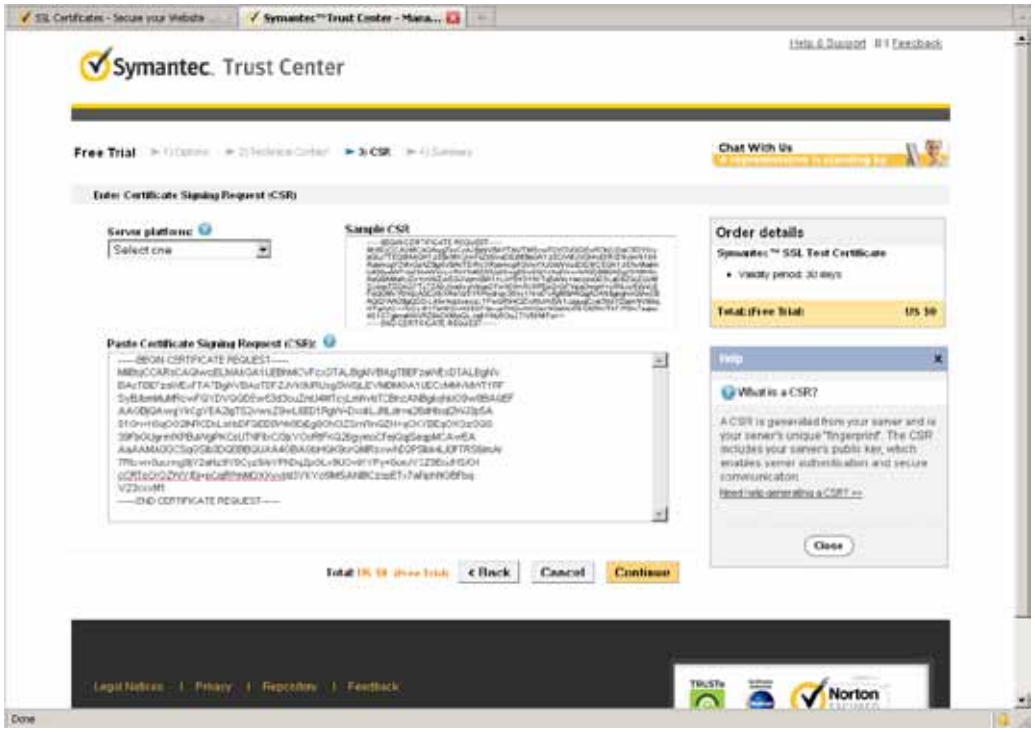
4. The Certificate request window will prompt.



If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.

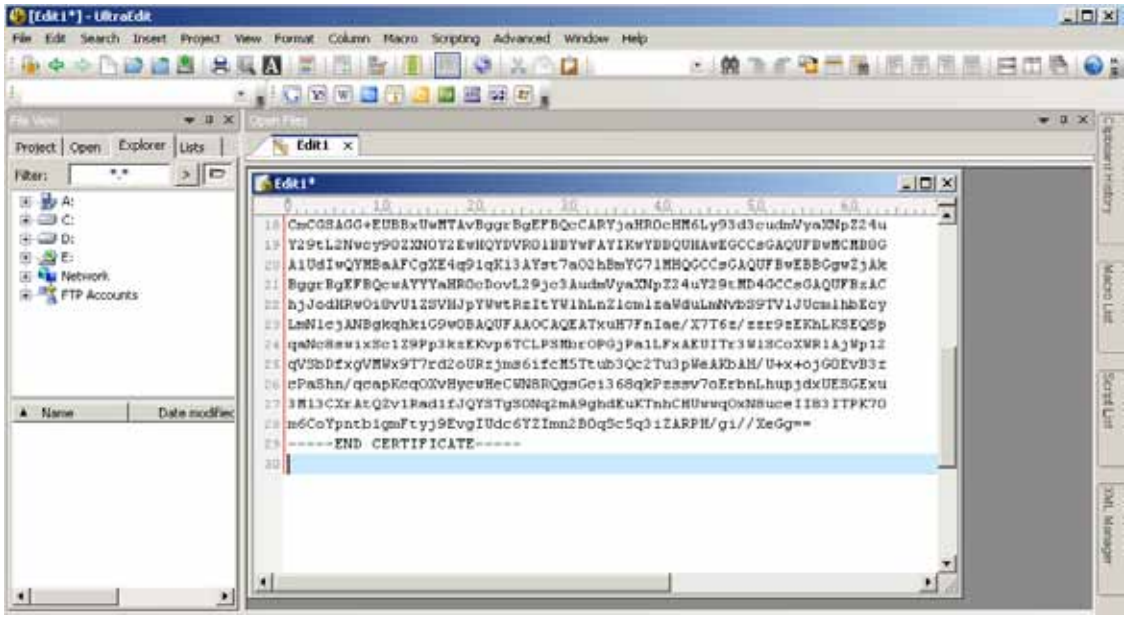


5. Look for a trusted certificate authority, such as Symantec's VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA's signing request window. Proceed with the rest of the process as CA's instructions on their webpage.

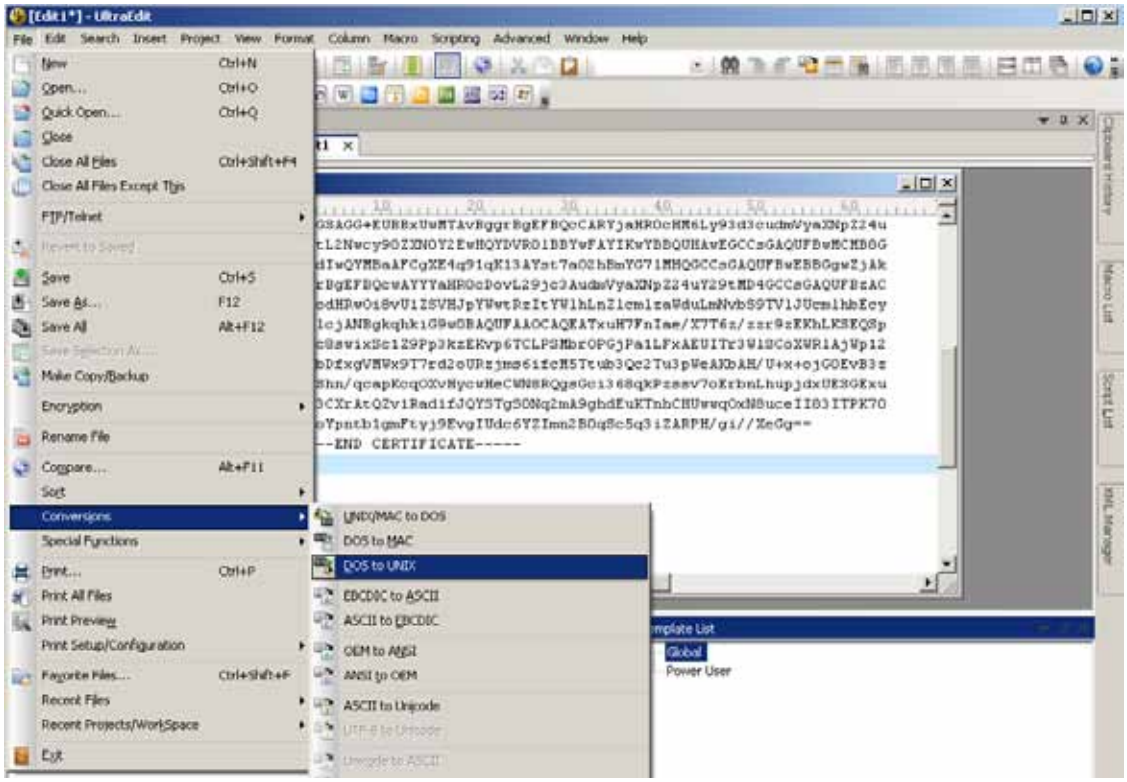


6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

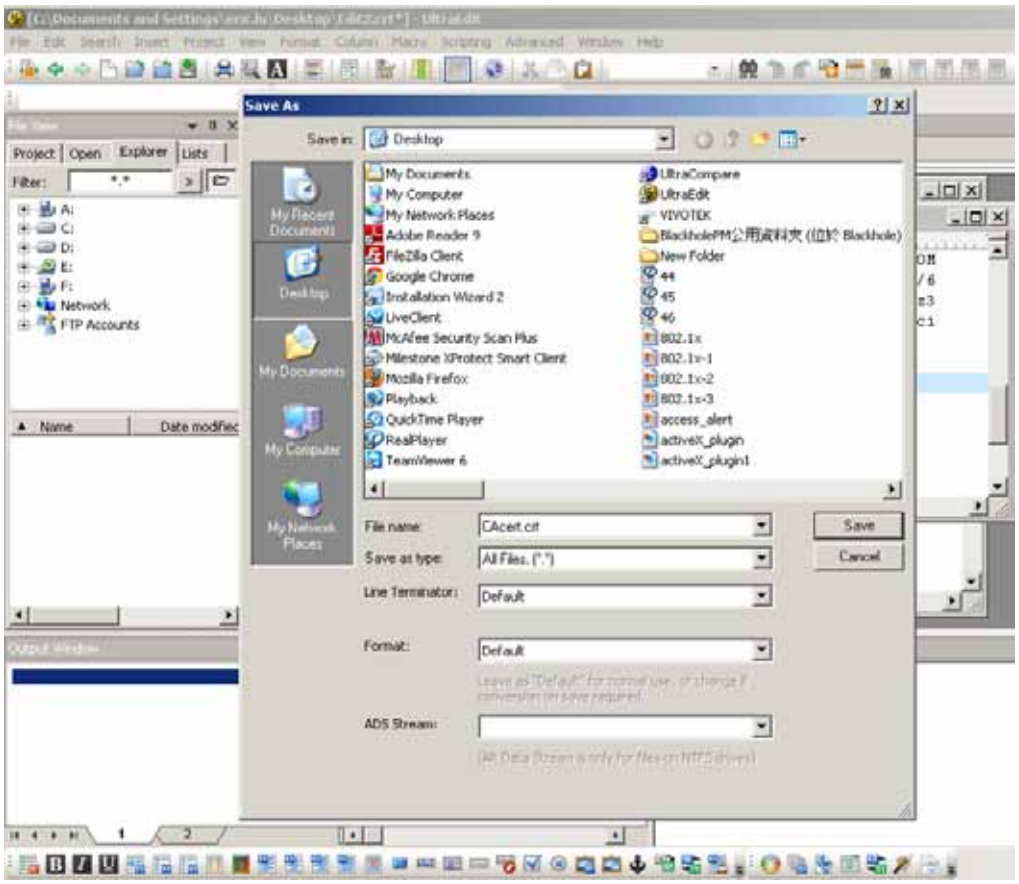
7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.



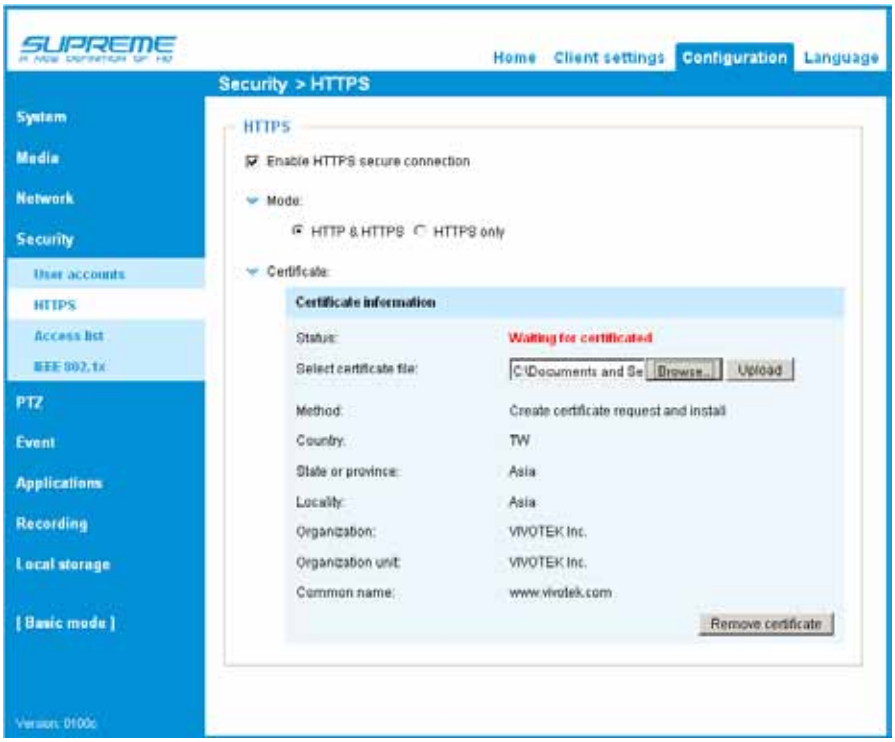
8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.



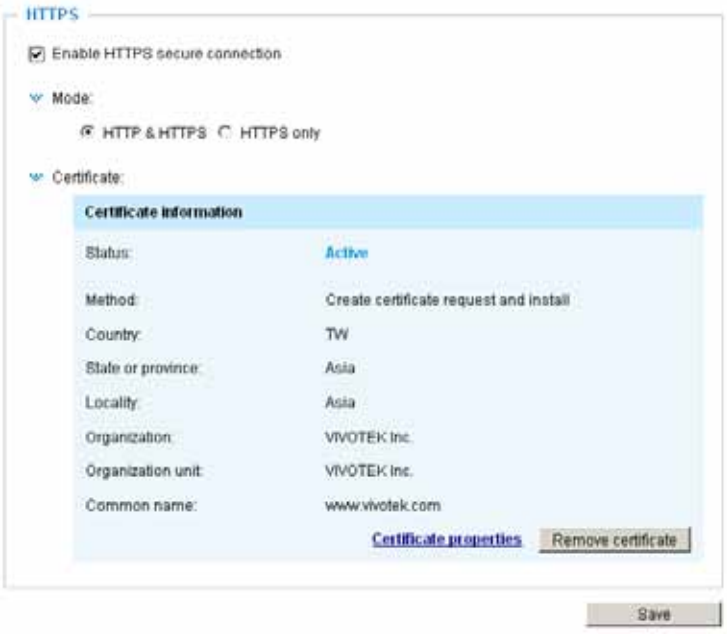
9. Save the edit using the ".crt" extension, using a file name like "CAcert.crt."



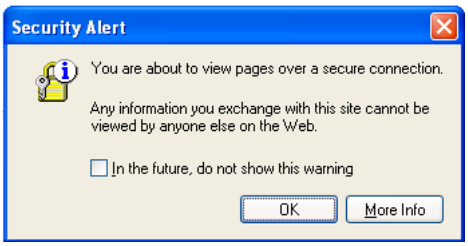
10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.

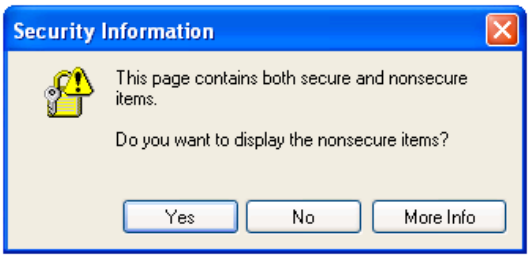


11. When the certifice file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the “**Save**" button for the configuration to take effect.



12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from “http://” to “https://“ in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

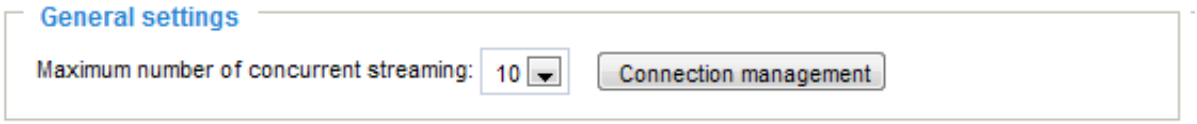




Security > Access List Advanced Mode

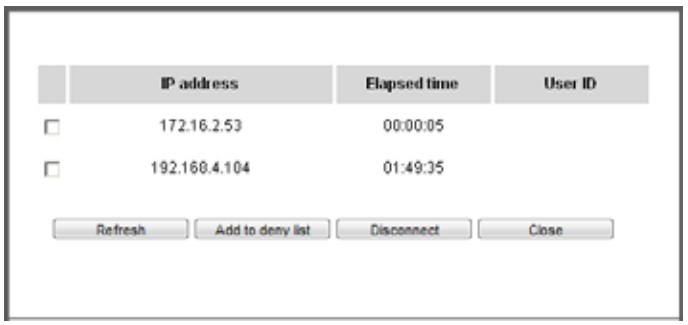
This section explains how to control access permission by verifying the client PC's IP address.

General Settings



Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

View Information: Click this button to display the connection status window showing a list of the current connections. For example:



Note that only consoles that are currently displaying live streaming will be listed in the View Information list.

■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations that allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 79.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 70.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to page 79.

■ Refresh: Click this button to refresh all current connections.

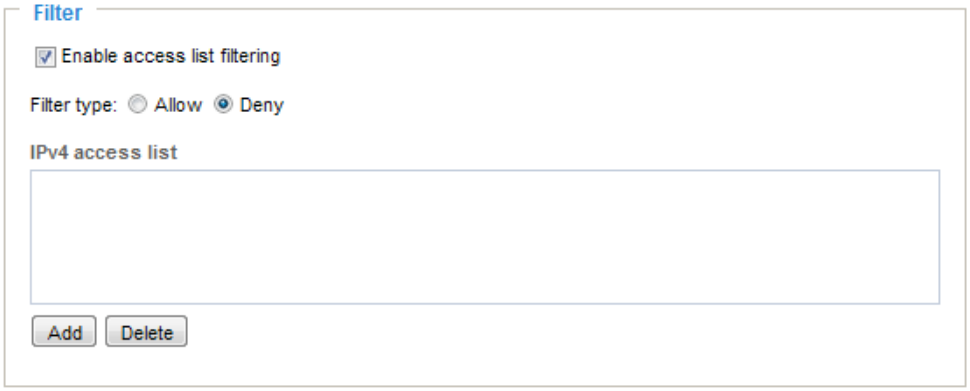
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explorer or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explorer or Quick Time Player).

Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

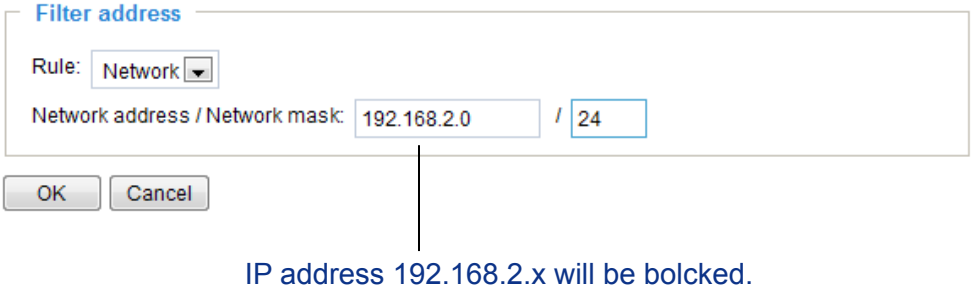
Filter type: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.



Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > General settings on page 62 for detailed information.

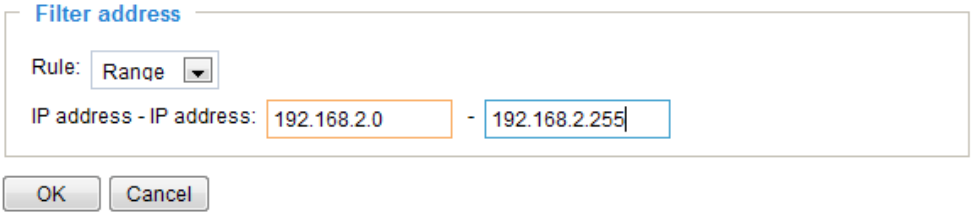
There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The address and network mask are written in CIDR format.
For example:



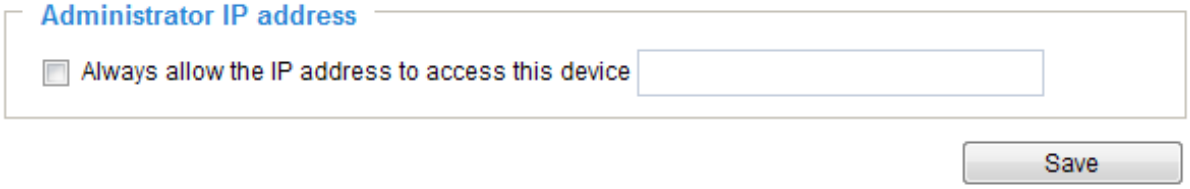
If IPv6 filter is preferred, you will be prompted by the following window. Enter the IPv6 address and the two-digit prefix length to specify the range of IP addresses in your configuration.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.
Note: This rule is only applied to IPv4.
For example:



Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



Security > IEEE 802.1X Advanced Mode

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

Supplicant
(Network Camera)

Authenticator
(Network Switch)

Authentication Server
(RADIUS Server)

1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A “go between” which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user’s access request.

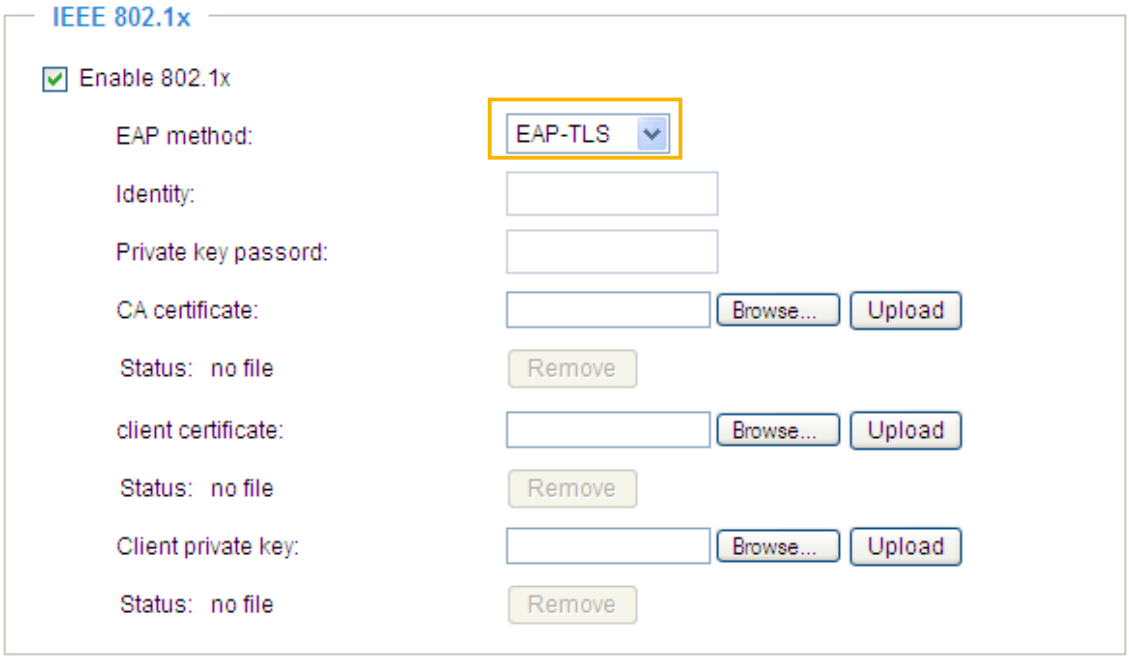
■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

IMPORTANT:

The maximum length of password is 200 symbols.

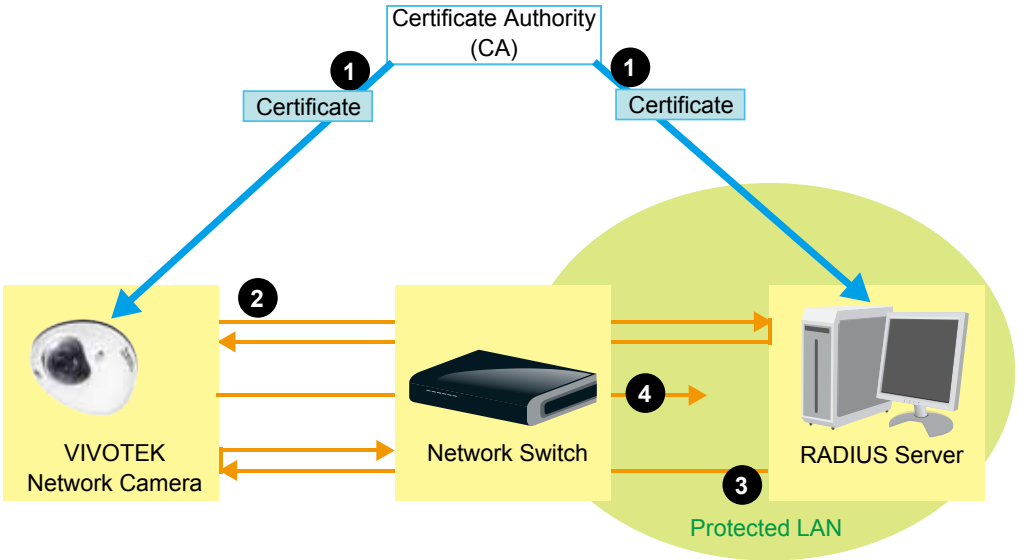


3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE:

► *The authentication process for 802.1x:*

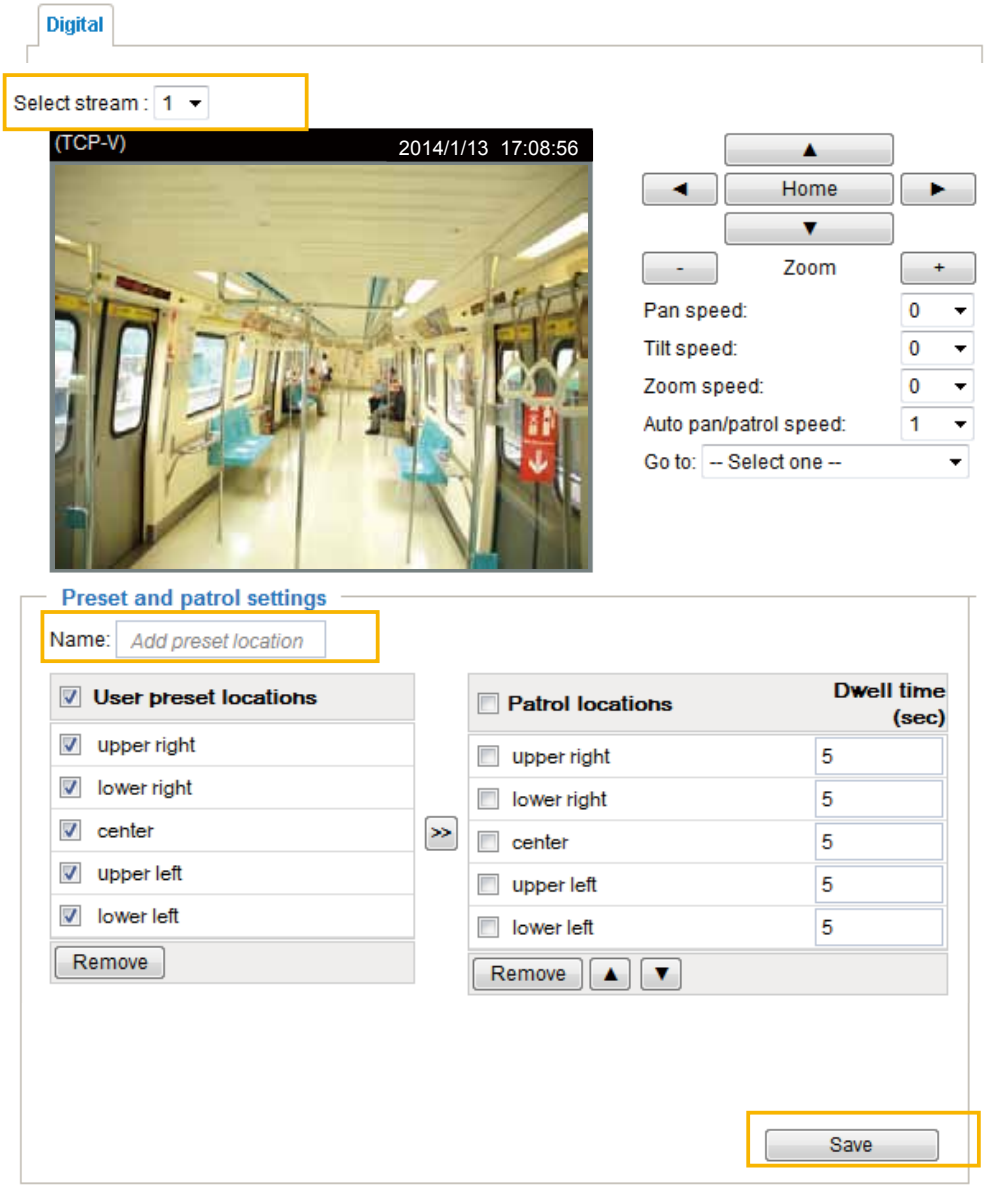
1. *The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).*
2. *A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the Network Camera.*
4. *Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.*



PTZ > PTZ settings Advanced Mode

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation. The e-PTZ fucntion allows users to quickly move the focus to a target area for close-up viewing without physically moving the camera. Please refer to below for detailed instruction.

Digital PTZ Operation (E-PTZ Operation)

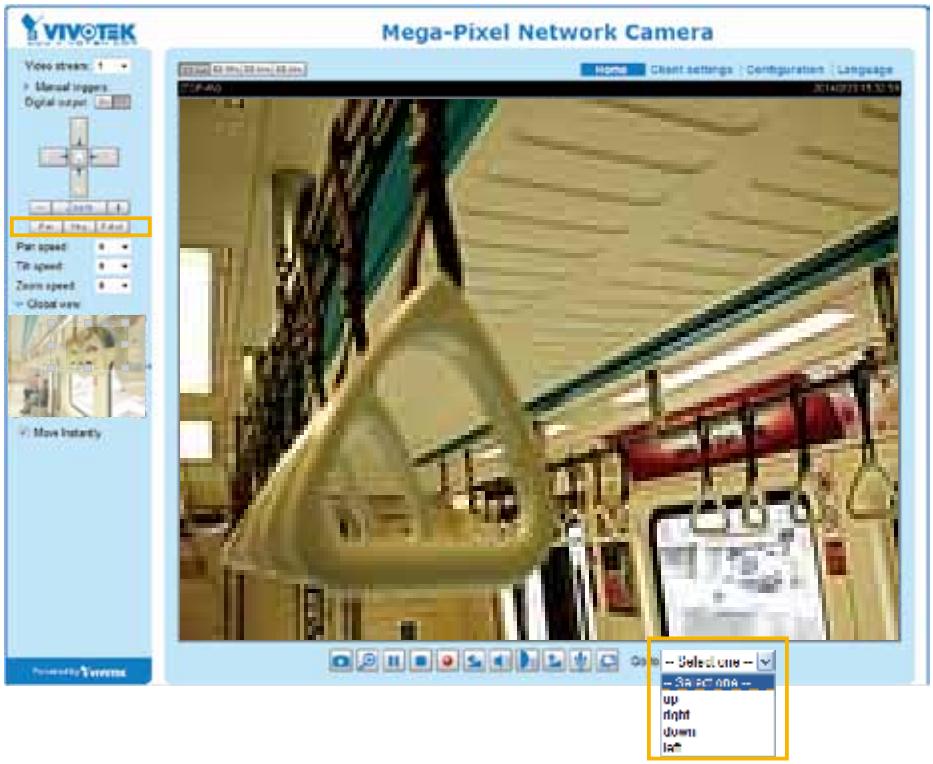


Select Stream: Select stream #1 to set up the e-PTZ control. Please note that each stream can possess its own preset and patrol settings. For detailed information about how to set up preset and patrol settings, please refer to page 93.

Auto pan/patrol speed: Select the speed from 1~5 (slow/fast) to set up the Auto pan/patrol speed control.

When completed with the e-PTZ settings, click **Save** to enable the settings on this page.

Home page in E-PTZ Mode



- The e-Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected e-preset position.
- If you have set up different e-preset positions for different streams, you can select one of the video streams to display its separate e-preset positions.

Global View

In addition to using the e-PTZ control panel, you can also use the mouse to drag or resize the floating frame to pan/tilt/zoom the viewing region. The live view window will also move to the viewing region accordingly.

Moving Instantly

If you check this item, the live view window will switch to the new viewing region instantly after you move the floating frame. If deselected, the process moving from one point to the other will be shown, yet it is not easy to observe if the move is not over a long distance.

Click on Image

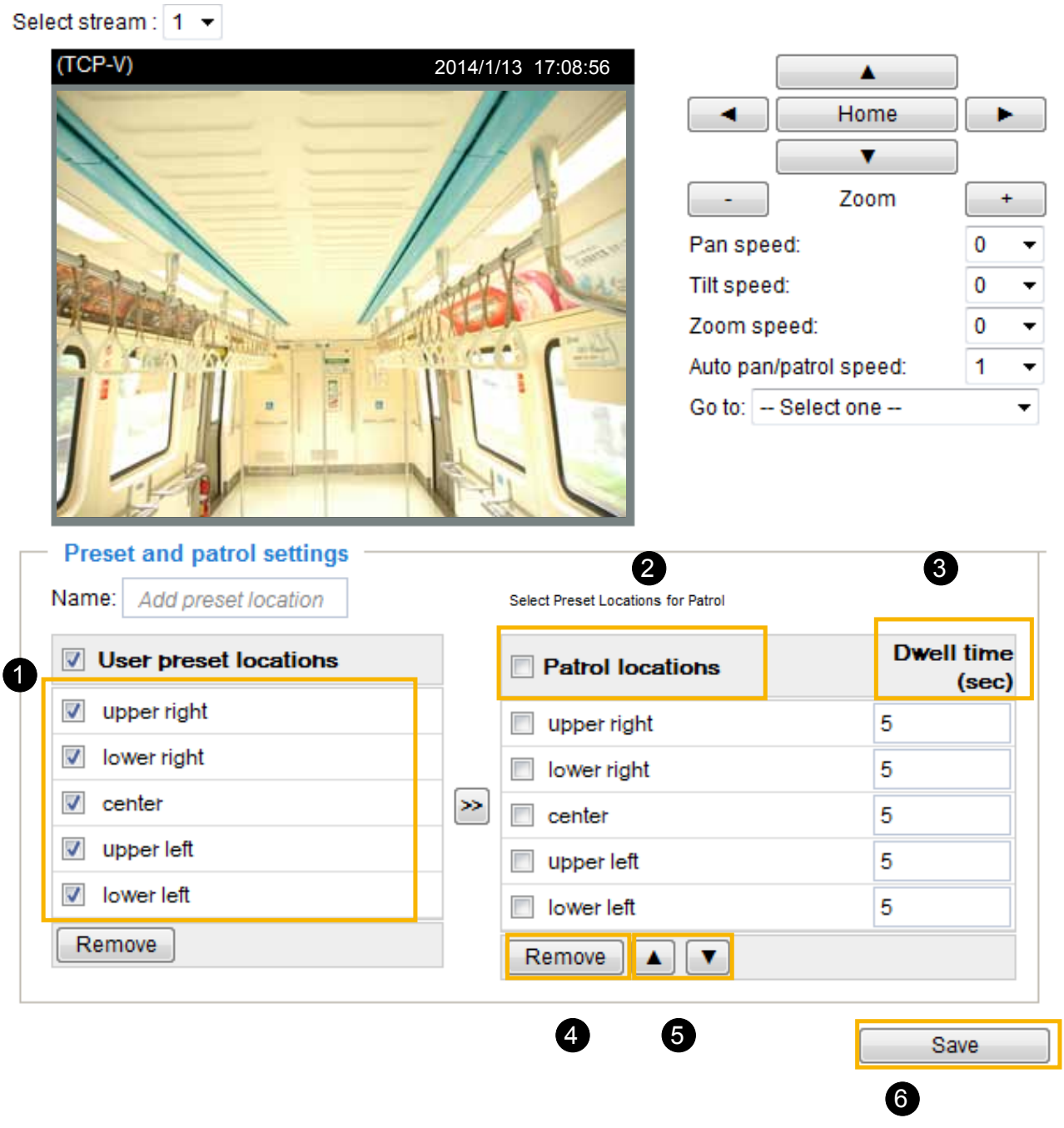
The e-PTZ function also supports “Click on Image“. When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point.

Note that the”Click on Image” function only applies when you have configured a smaller “Region of Interest” out of the maximum output frame! e.g., a 800x600 region from a 1280x960 frame size.

Patrol settings

You can select some preset positions for the Network Camera to patrol.
Please follow the steps below to set up a patrol schedule:

1. Select the preset locations on the list, and click >>.
2. The selected preset locations will be displayed on the **Patrol locations** list.
3. Set the **Dwelling time** for the preset location during auto patrol.
4. If you want to delete a preset location from the Patrol locations list, select it and click **Remove**.
5. Select a location and click ▲ ▼ to rearrange the patrol order.
6. Select patrol locations you want to save in the list and click **Save** to enable the patrol settings.
7. To implement the patrol schedule, please go to homepage and click on **Patrol** button. Please refer to the next page.



Home page in the e-PTZ Mode

The **Preset positions** will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected preset position.

Patrol button: Click this button, then the Network Camera will patrol among the selected preset positions continuously.

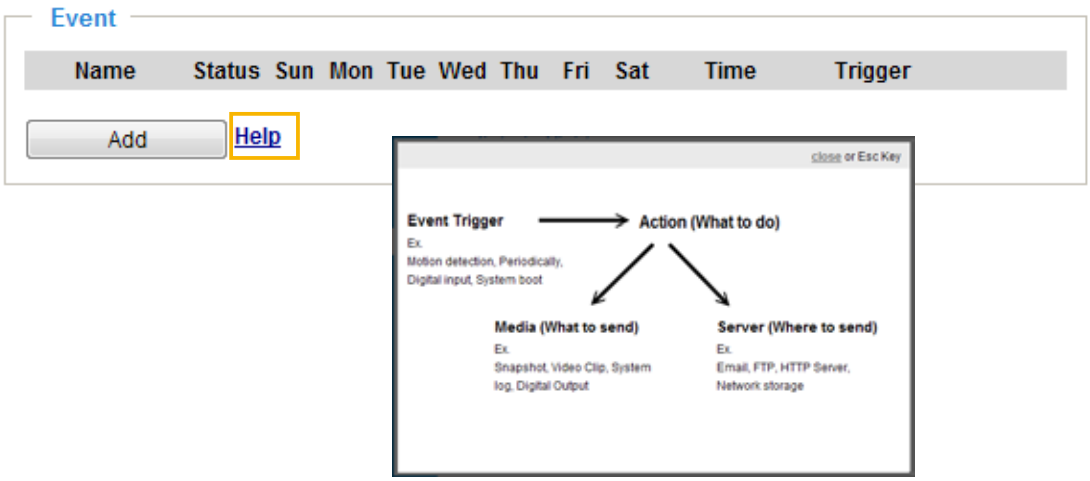
NOTE:

► *The Preset Positions will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected preset position.*

► *Click Patrol: The Network Camera will patrol along the selected positions repeatedly. Please refer to page 95 to see more details.*

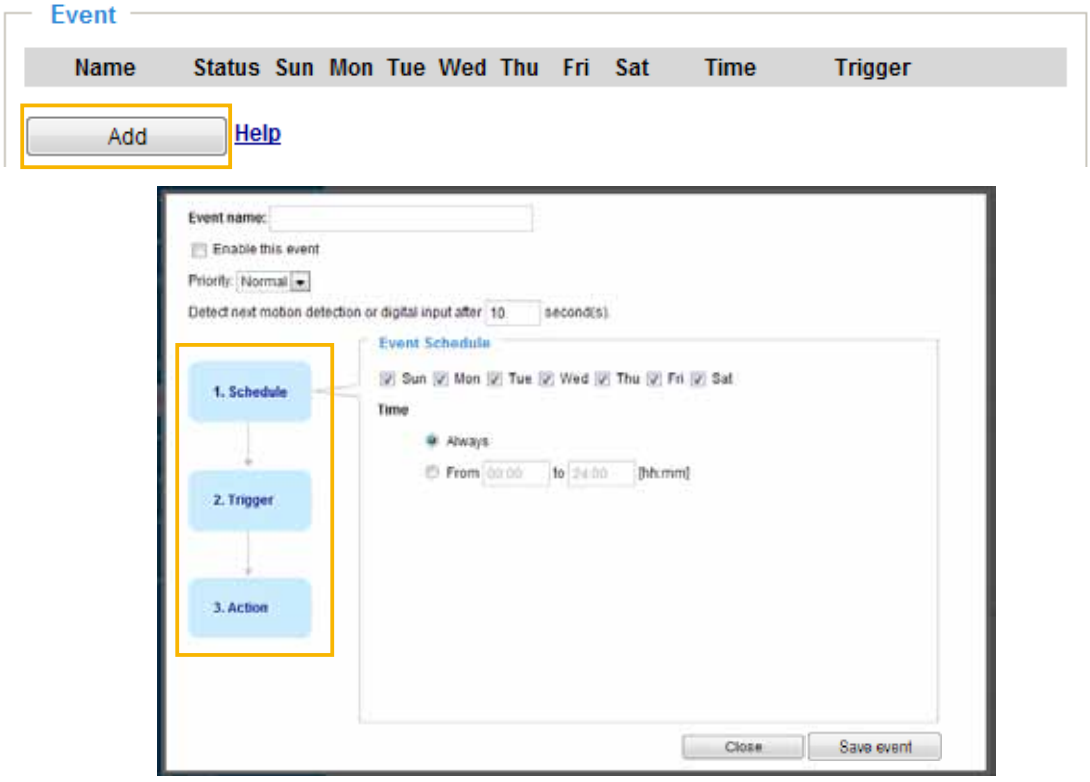
Event > Event settings Advanced Mode

This section explains how to configure the Network Camera to respond to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.



Event

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window. Here you can arrange three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.



■ Event name: Enter a name for the event setting.

■ Enable this event: Select this option to enable the event setting.

■ Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

■ Detect next motion detection or digital input after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected. This can prevent event-related actions to be too frequently performed.

1. Schedule

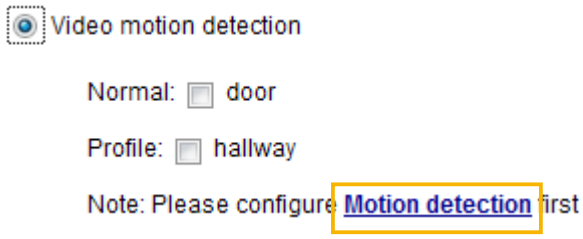
Specify the period of time during which the event trigger will take place. Please select the days of the week and the time in a day (in a 24-hr time format) for the event triggering schedule.

2. Trigger

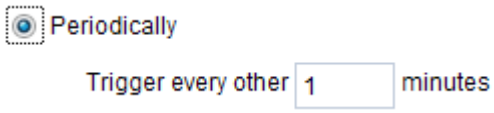
This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources as shown on next page. Select the item to display the detailed configuration options.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 111 for details.



■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.



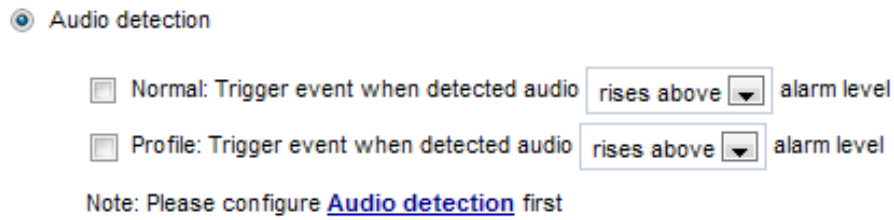
■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which help detect changes in temperature, vibration, sound, and light, etc.

■ System boot
This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data.

■ Audio detection

A preset threshold can be configured with an external microphone as the trigger to system event. The triggering condition can be an input exceeding or falling below a threshold. Audio detection can take place as a complement to motion detection or as a method to detect activities not covered by the camera's view.



Once you have a preset audio alarm level, you can define the triggering condition either as an audio input rises above or falls below the alarm level.

■ Temperature detection

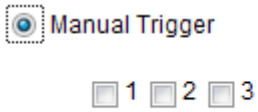
Whenever the detected temperature breaches the high (upper) or low (lower) threshold, the breach can be used as a triggering condition. The camera comes with an onboard temperature sensor, and the thresholds can be configured in Application > Temperature detection.

■ Camera tampering detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 114 for detailed information.

■ Manual Trigger

This option allows users to enable event triggers manually by t on the homepage. Please configure 1 to 3 associated events before using t

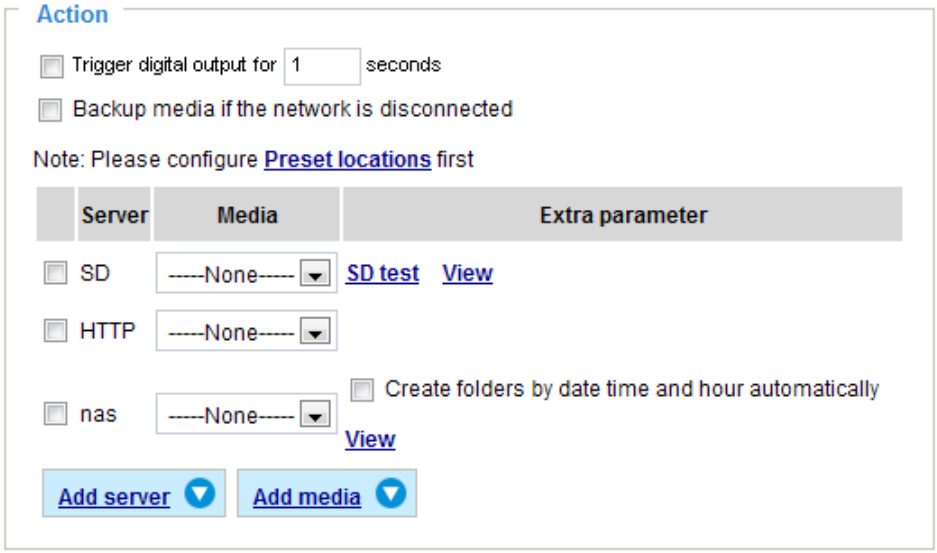


■ VADP (VIVOTEK Application Development Platform)

The triggering conditions detected by 3rd-party software modules, such as motion detection or line-crossing (tripwire), can also be used as event triggers.

3. Action

Define the actions to be performed by the Network Camera when a trigger is activated.



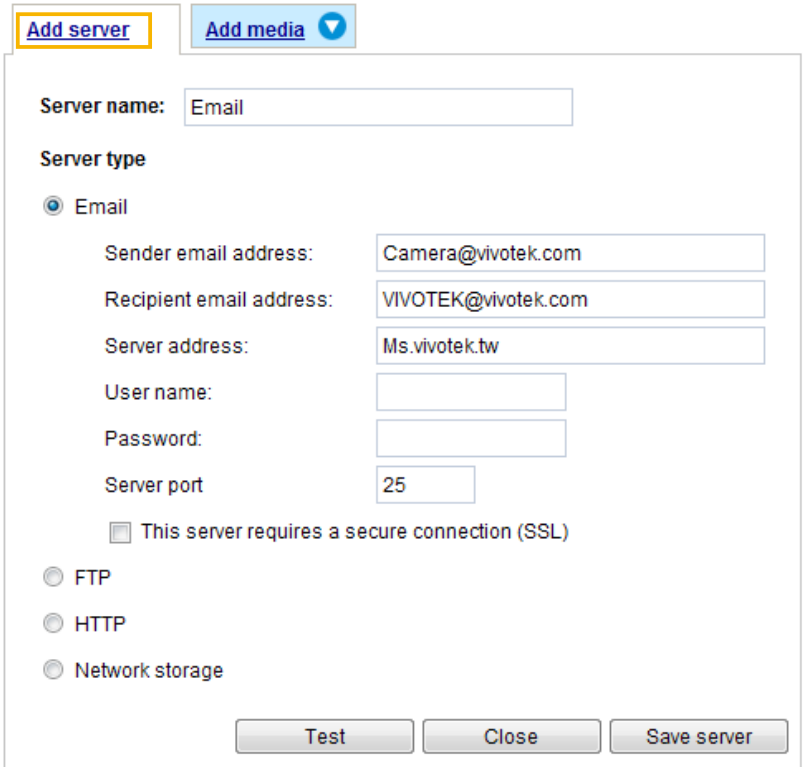
■ Trigger digital output for __ second(s)
If selected, when an event is triggered, the camera will trigger the digital output signal for configurable period of time. The output signal can then be used to turn on another device, such as an illuminator.

■ Backup media if the network is disconnected
Select this option to backup media file on SD card if the network is disconnected. This function will only be displayed after you set up a networked storage (NAS).

Add server

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. Click **Add server** to open the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.



Server type - Email
Select to send the media files via email when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

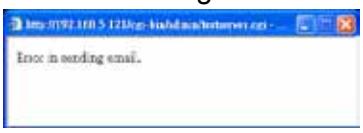
■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

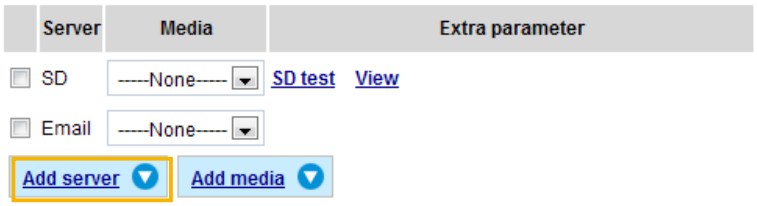
If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.



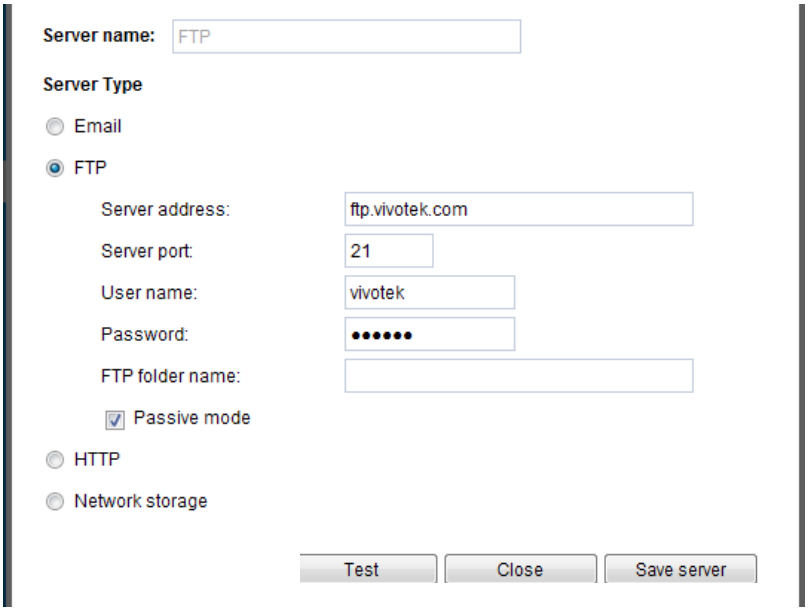
Click **Save server** to enable the settings.

Note that after you set up the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.



Server type - FTP

Select to send the media files to an FTP server when a trigger is activated.



■ Server name: Enter a name for the server setting.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

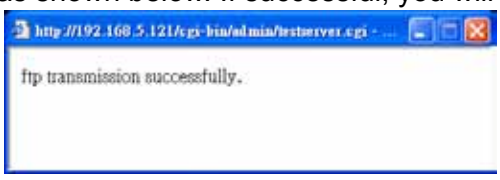
■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will automatically create one on the FTP server.

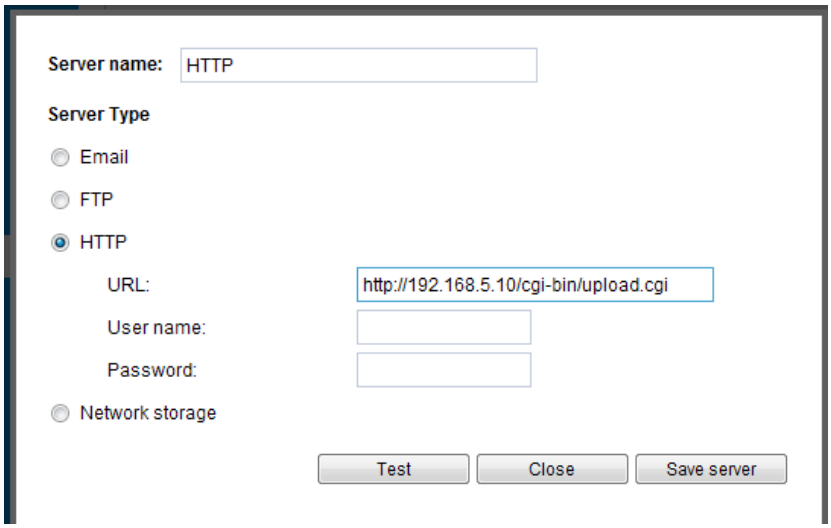
■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall. The firmware default has the Passive mode checkbox selected.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.



Click **Save server** to enable the settings.

Server type - HTTP
Select to send the media files to an HTTP server when a trigger is activated.



■ Server name: Enter a name for the server setting.

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

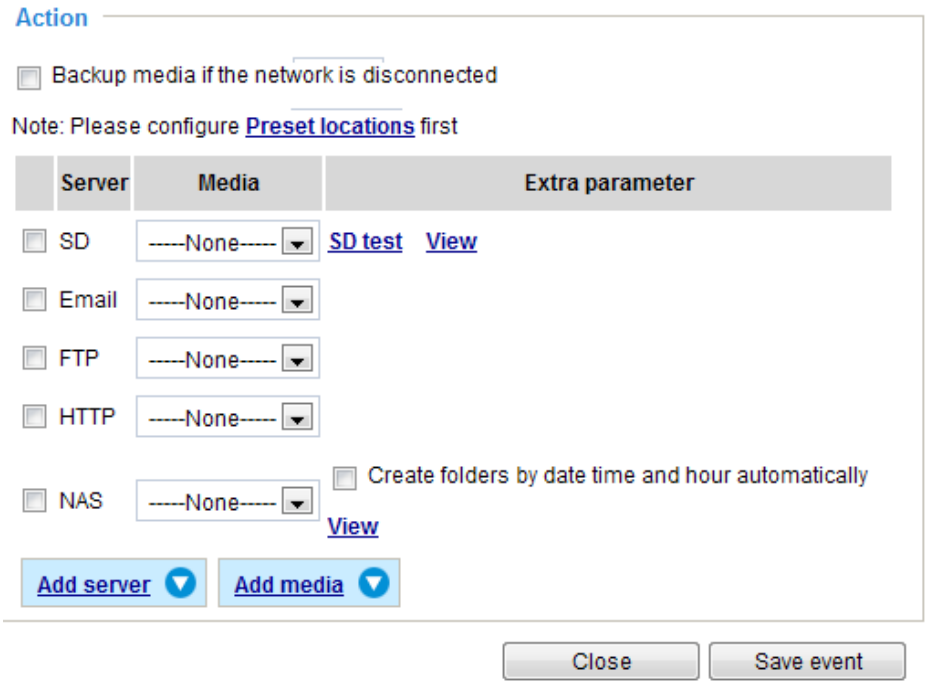
■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.

Click **Save server** to enable the settings.

Network storage:
Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 122 for details.

Click **Save server** to enable the settings.

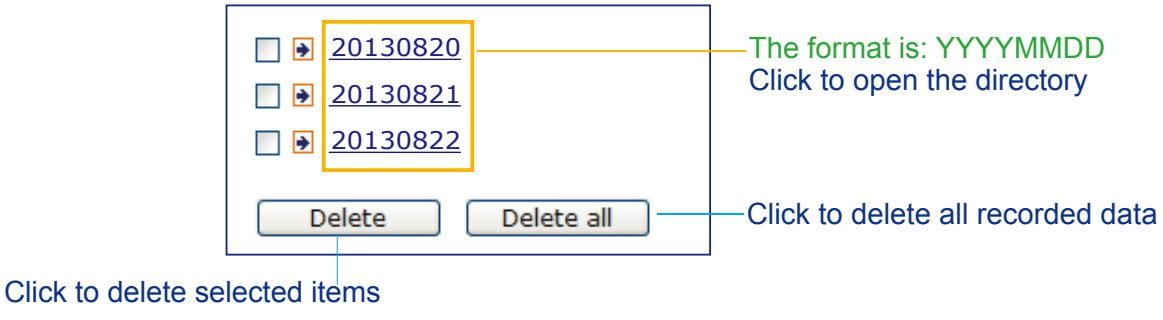


- SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 125 for detailed information.

- View: Click this button to open a file list window. This function is only for SD card and Network Storage. If you click the View button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 125. If you click the View button of Network storage, a file directory window will pop up for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.

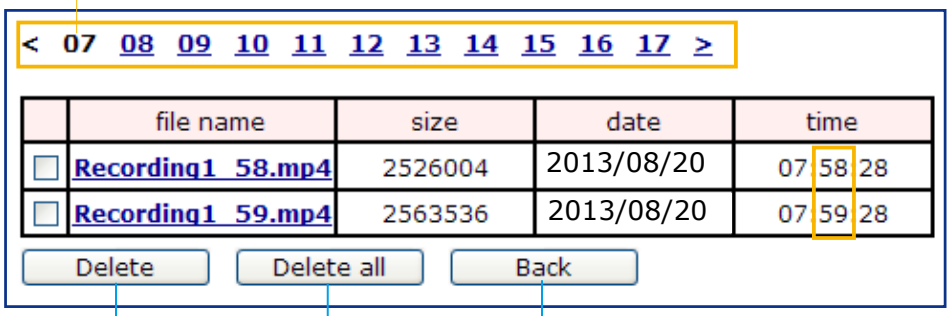
- Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by the date when video footages are stored onto the networked storage.

The following is an example of a file destination with video clips:



Click **20130820** to open the directory:

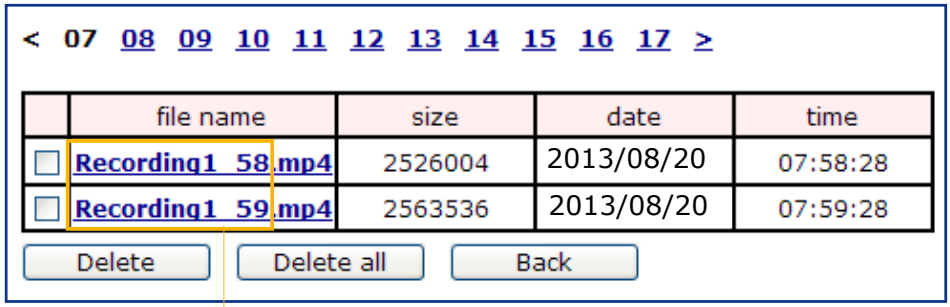
The format is: HH (24r)
Click to open the file list for that hour



Click to delete selected items

Click to delete all recorded data

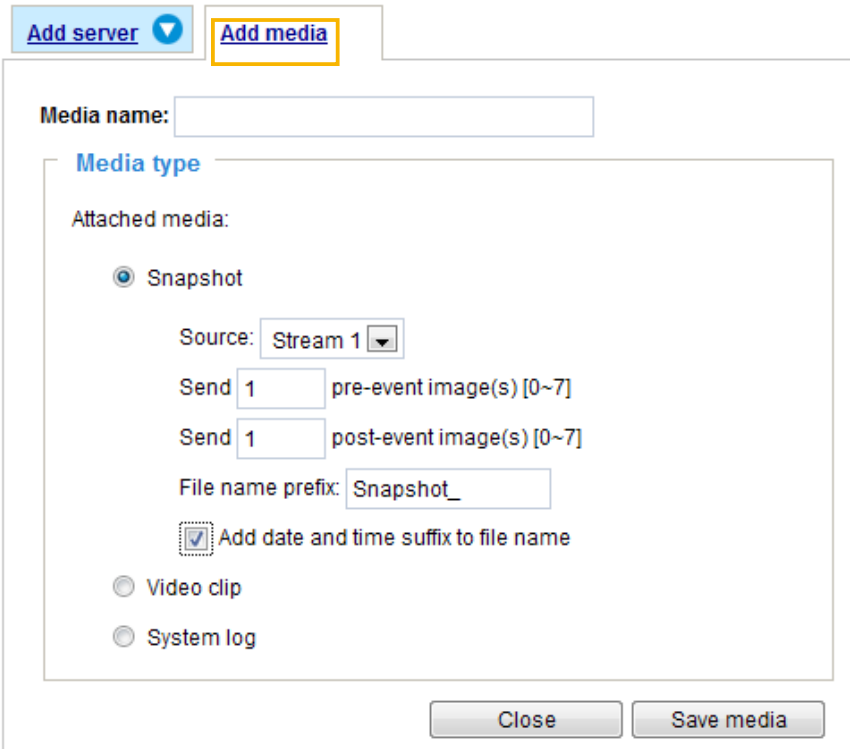
Click to go back to the previous level of the directory



The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Add media page. Please refer to next page for detailed information.

Add media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.



Media type - Snapshot
Select to send snapshots when a trigger is activated.

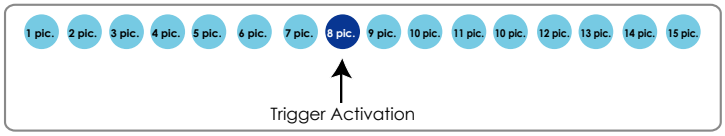
■ Media name: Enter a name for the media setting.

■ Source: Select to take snapshots from a video stream.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

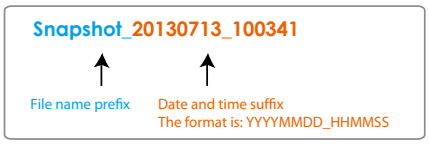
■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



■ File name prefix
Enter the text that will be appended to the front of the file name.

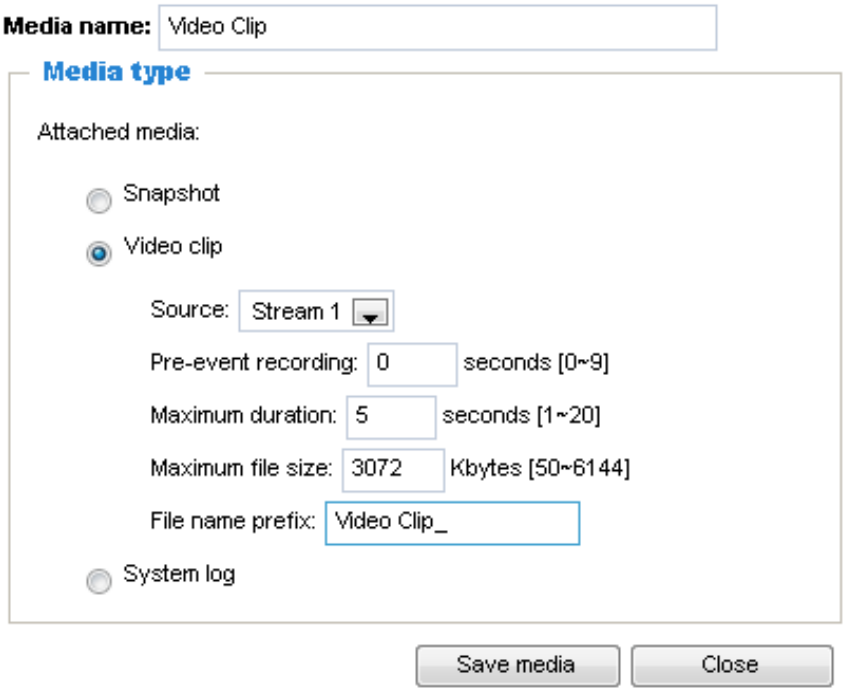
■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:



Click **Save media** to enable the settings.

To note that after you set up the first media server, a new column for media server will automatically show up on the Media list. If you wish to add more other media options, click **Add media**.

Media type - Video clip
Select to send video clips when a trigger is activated.

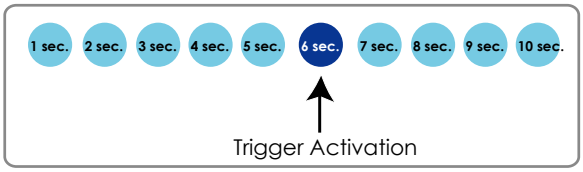


■ Media name: Enter a name for the media setting.

■ Source: Select the source of video clip.

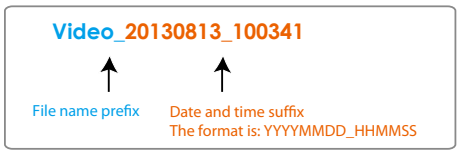
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



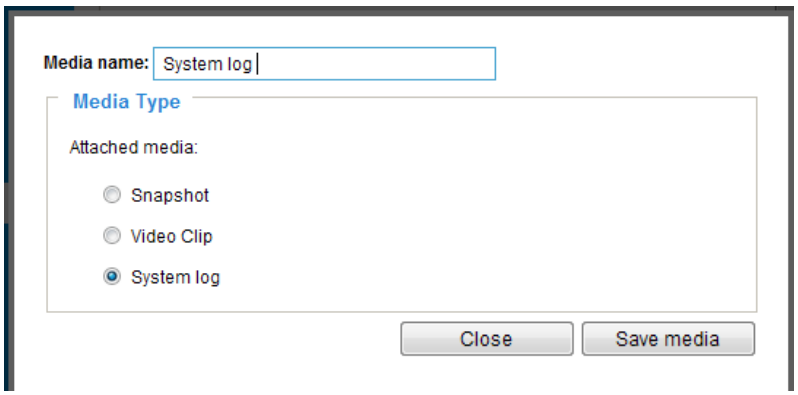
■ Maximum file size
Specify the maximum file size allowed.

■ File name prefix
Enter the text that will be appended to the front of the file name.
For example:

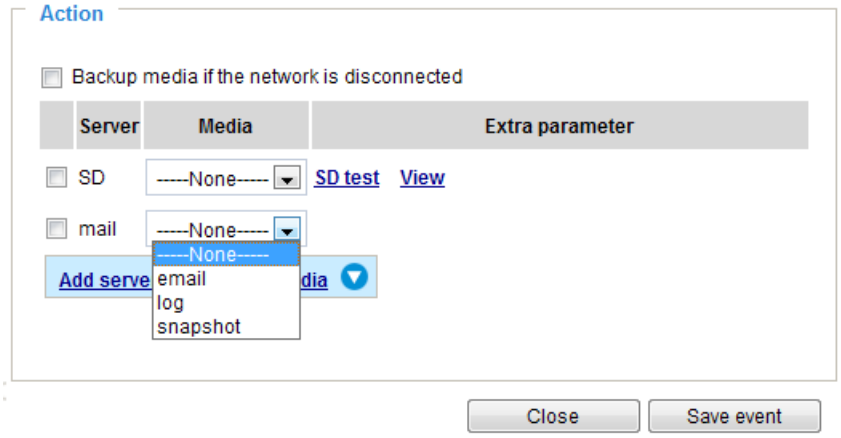


Click **Save media** to enable the settings.

Media type - System log
Select to send a system log when a trigger is activated.



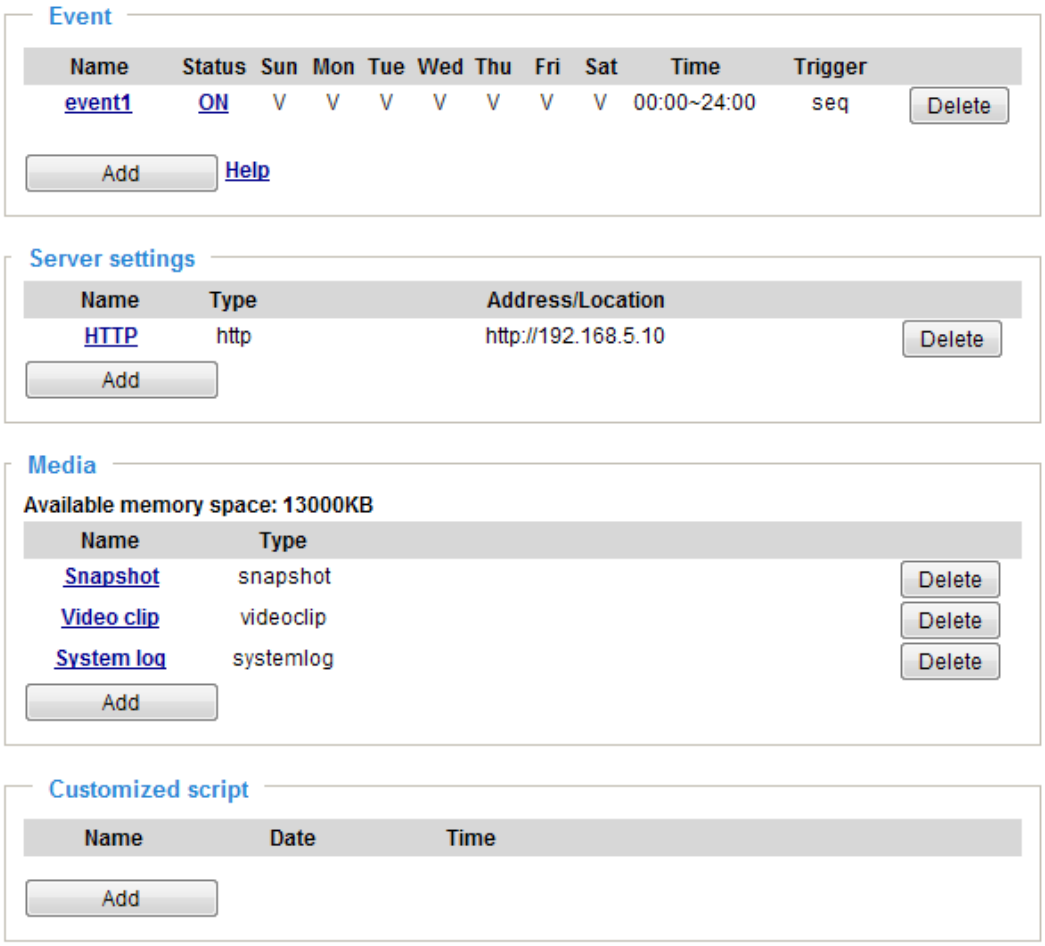
Click **Save media** to enable the settings, then click **Close** to exit the page.



In the Event settings column, the Servers and Medias you configured will be listed; please make sure the Event -> Status is indicated as **ON**, in order to enable the event triggering action.

When completed, click **Save event** to enable the settings and click **Close** to exit Event Settings page. The new Event / Server settings / Media will appear in the event drop-down list on the Event setting page.

Please see the example of the Event setting page below:



When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

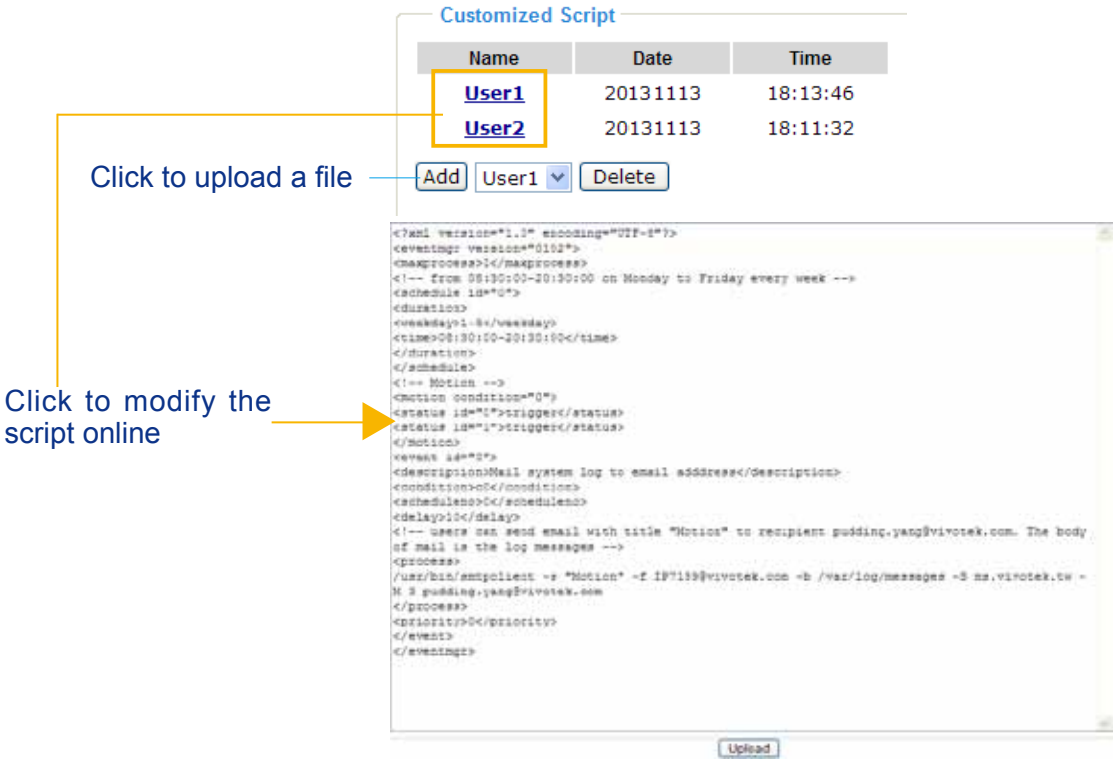
If you want to stop the event trigger, you can click on the **ON** button to turn its status to **OFF** or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that you can only delete a server setting when it is not applied to an existing event setting.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that you can only delete a media setting when it is not applied to an event setting.

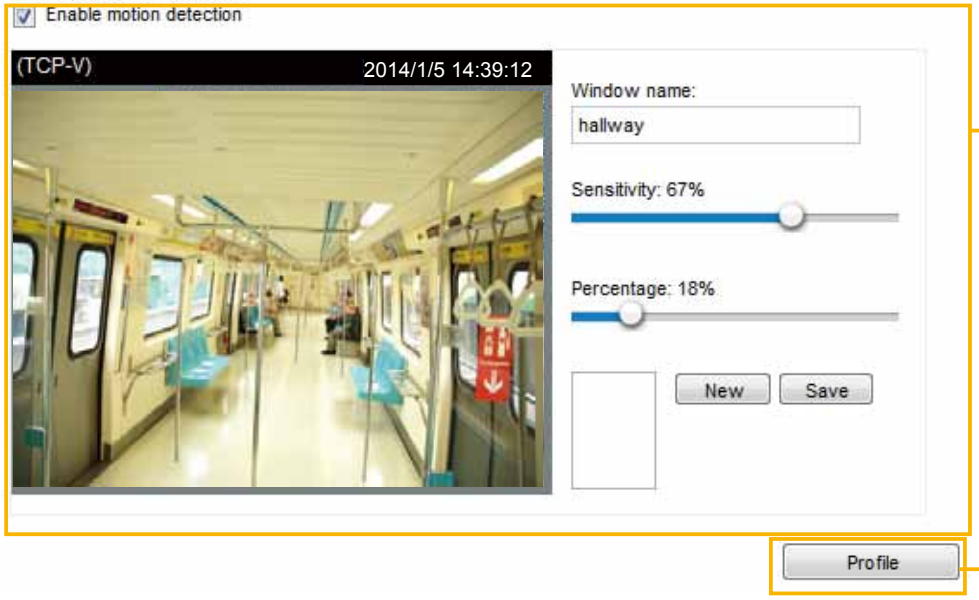
Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt. If you need more information, please contact VIVOTEK technical support.



Applications > Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



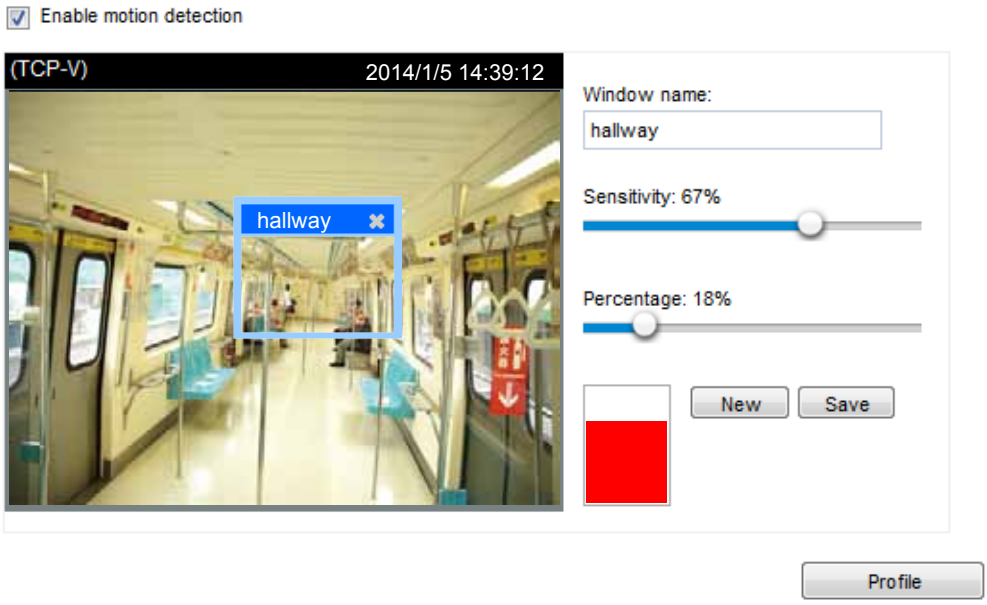
Motion Detection Setting 1: For normal situations

Motion Detection Setting 2: For special situations

Follow the steps below to enable motion detection:

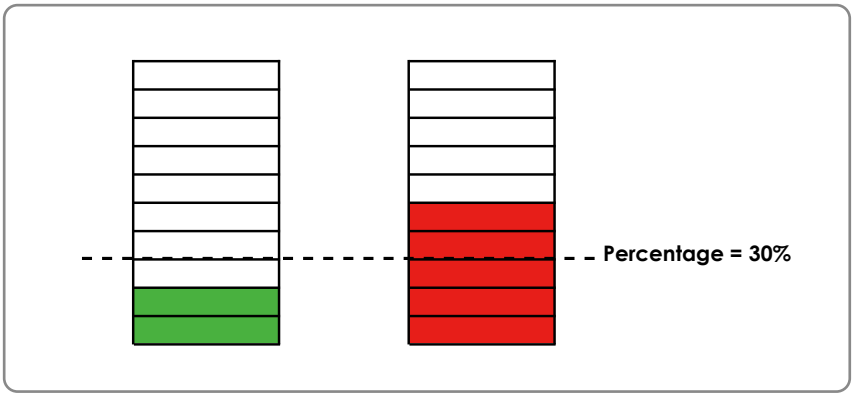
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   - To move and resize the window, drag and drop your mouse on the window.
   - To delete a window, click X on the upper right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slide bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:



The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Event settings on page 97.

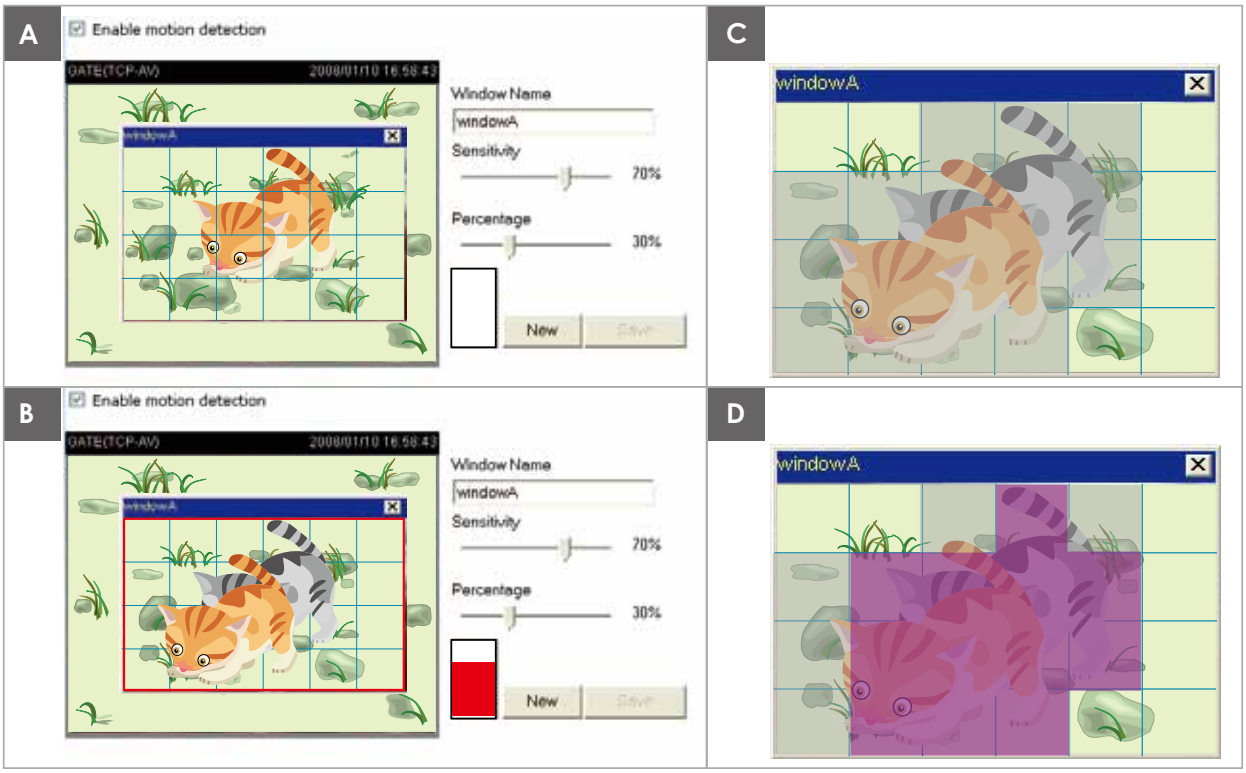
A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



This motion detection window will also be displayed on the Event Settings page. You can go to Event > Event settings > Trigger to choose it as a trigger source. Please refer to page 121 for detailed information.

NOTE:

► *How does motion detection work?*

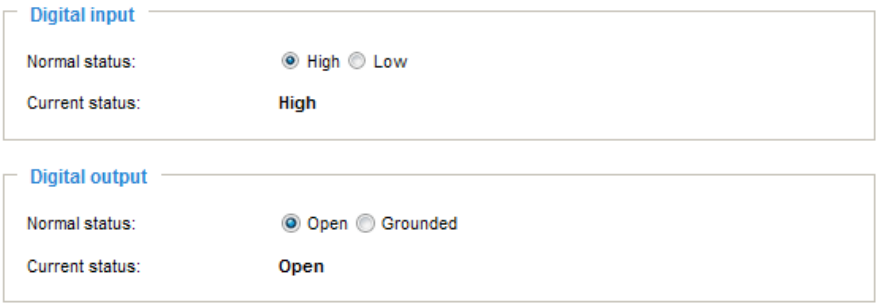


There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

Applications > DI and DO Advanced Mode



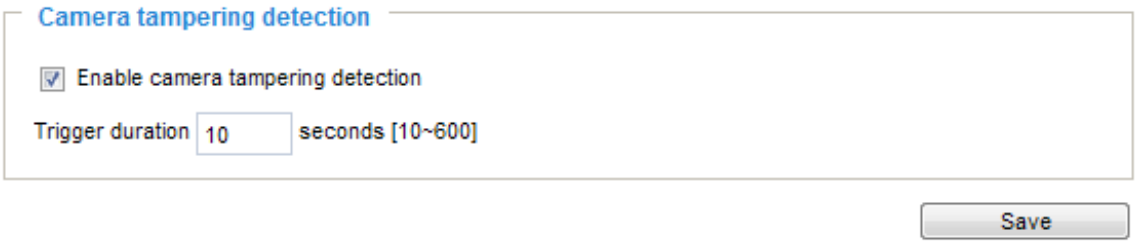
Connect DI devices to the camera's terminal block, the camera will automatically detect the current connection state as pulled-high or pulled-low. You may then define the triggering condition.

Digital input: Select High or Low to define the "active state" for the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define the "active state" for the digital output. The Network Camera will show whether the trigger is activated or not.

Applications > Tampering detection

This section explains how to set up camera tamper detection. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.

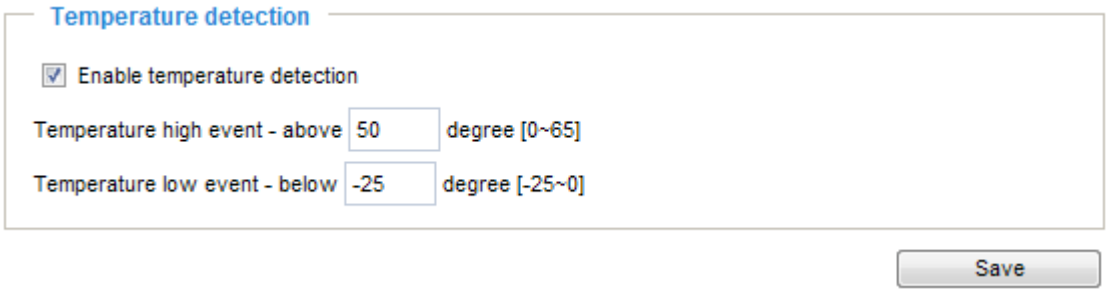


Please follow the steps below to set up the camera tamper detection function:

1. Check **Enable camera tampering detection**.
2. The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Event > Event settings > Trigger.** Please refer to page 121 for detailed information.

Applications > Temperature detection

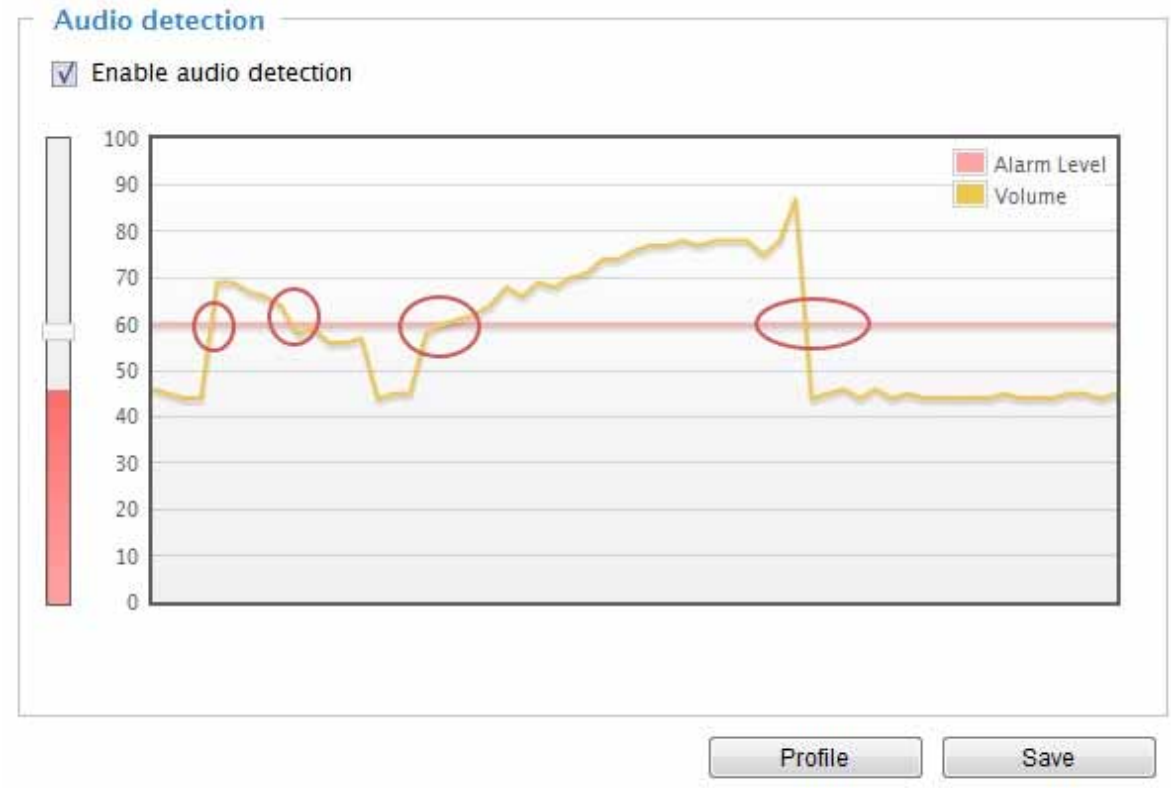
The camera comes with an onboard temperature sensor. You can configure the high (upper) or low (lower) thresholds for the sensor. If you enable temperature detection, and when any of the threshold values is breached, system alarms will be issued. You can configure the responsive action, such as sending system logs via Email, in Event > Event settings. The temperature alarms can be applied as one of the triggering conditions.



Applications > Audio detection Advanced Mode

Audio detection, along with video motion detection, is applicable in the following scenarios:

1. Detection of activities not covered by camera view, e.g., a loud input by gun shots or breaking a door/window.
2. A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines.
3. A PTZ camera can be directed to turn to a preset point by the occurrence of audio events.
4. Dark environments where video motion detection may not function well.



The red circles indicate where the audio alarms can be triggered when breaching or falling below the preset threshold.

How to configure Audio detection:

1. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
2. Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.
3. Select the “Enable audio detection“ checkbox and click Save to enable the feature.

NOTE:

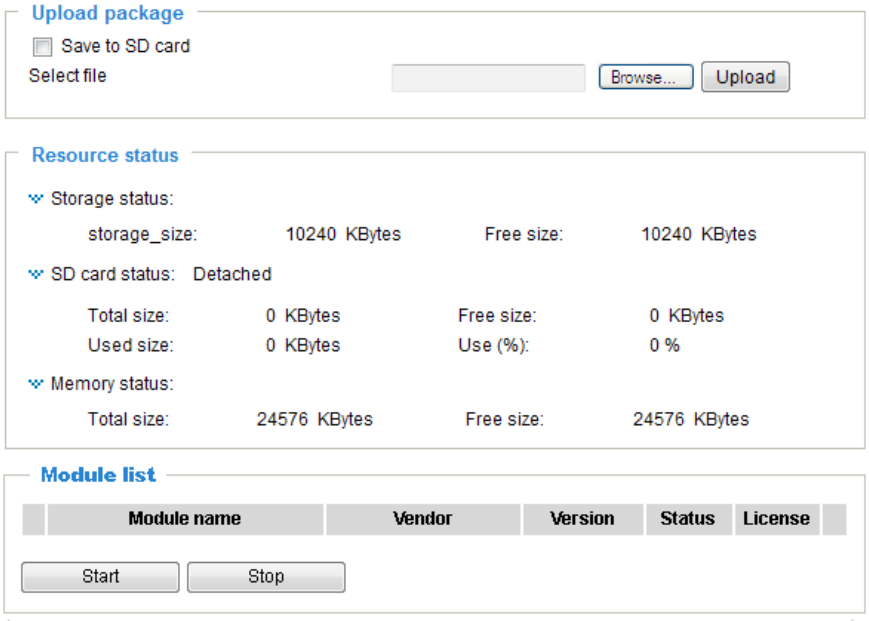
1. *Note that the volume numbers (0~100) on the side of wave diagram does not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.*

2. *To configure this feature, you must not mute the audio in* **Configuration > Media > Audio**. *The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.*

IMPORTANT:

- If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.
- To configure and enable this feature, you **must not** configure video stream #1 into **Motion JPEG**. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station **along with stream #1**.
- Refer to page 61 for Audio settings, and page 55 for video streaming settings.

Applications > VADP (VIVOTEK Application Development Platform)



Users can store and execute VIVOTEK's or 3rd-party software modules onto the camera's flash memory or SD card. These software modules can apply in video analysis for intelligent video applications such as license plate recognition, object counting, or as an agent for edge recording, etc.

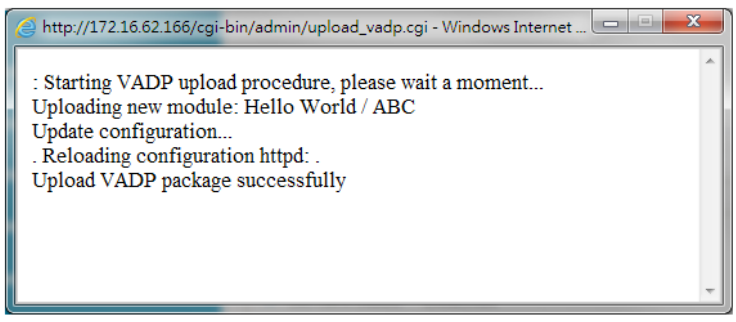
- Once the software package is successfully uploaded, the module configuration (vadp.xml) information is displayed. When uploading a module, the camera will examine whether the module fits the predefined VADP requirements. Please contact technical support or the vendor of your 3rd-party module for the parameters contained within.

- Users can also run VIVOTEK's VADP packages as a means to access updated functionality instead of replacing the entire firmware.

- Note that for some cameras the flash is too small to hold VADP packages. These cameras will have its "Save to SD card" checkbox selected and grayed-out for all time.

- The file system of SD card (FAT32) does not support soft (symbolic) link. It will return failure if your module tries to create soft links on SD card.

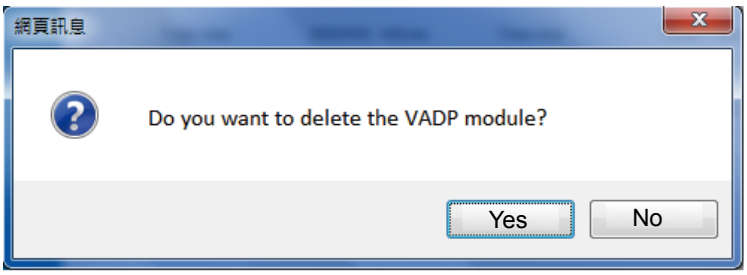
To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons. The screen message for a successful upload is shown below:



To start a module, select the checkcircle in front, and click the **Start** button.

If you should need to remove a module, select the checkcircle in front and then click the **Stop** button. By then the module status will become **OFF**, and the **X** button will appear at the end of the row. Click on the **X** button to remove an existing module.

When prompted by a confirm message, Click **Yes** to proceed.

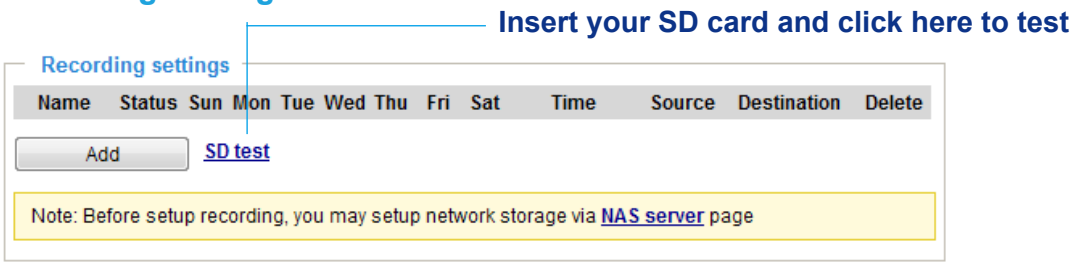


Note that the actual memory consumed while operating the module will be indicated on the **Memory status** field. This helps determine whether a running module has consumed too much of system resources.

Recording > Recording settings Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

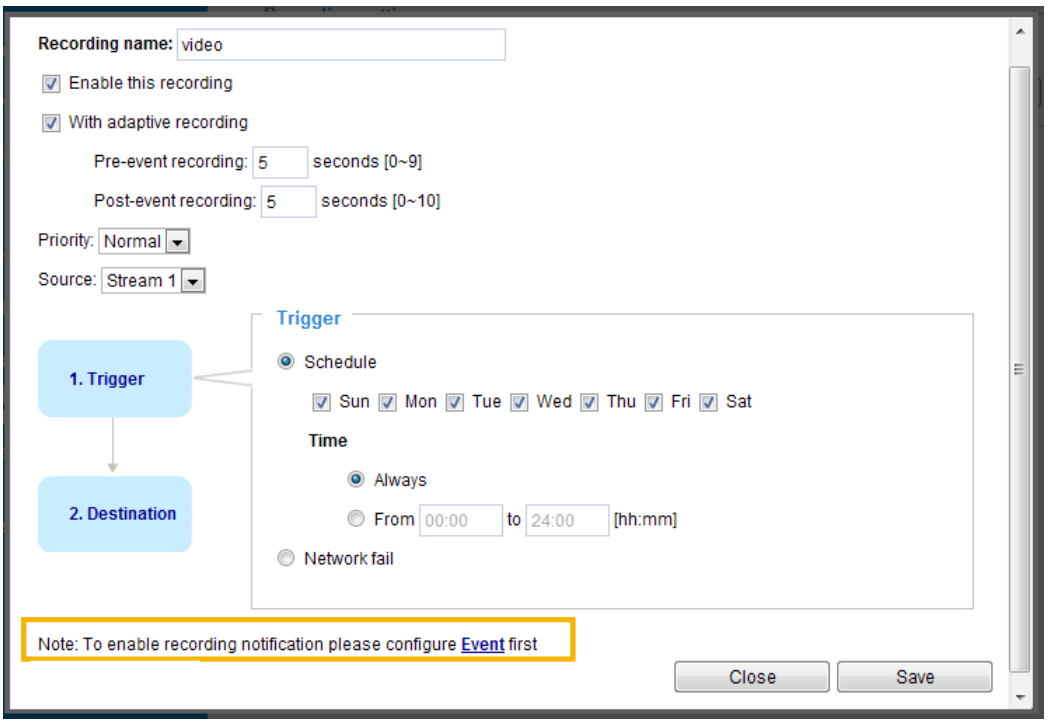


NOTE:

► *Please remember to format your SD card when using it for the first time. Please refer to page 125 for detailed information.*

Recording Settings

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

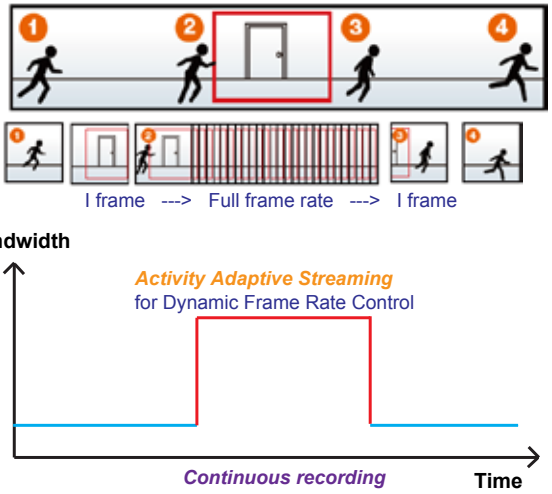


■ Recording name: Enter a name for the recording setting.

■ Enable this recording: Select this option to enable video recording.

■ With adaptive recording:
Select this option will activate the frame rate control according to alarm trigger.
The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've set on Video quality page. Please refer to page 58 for more information.

If you enable adaptive recording and enable time-shift cache stream on Camera A, only when an event is triggered on Camera A will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidths and storage space.



NOTE:

► *To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.*

► *When there is no alarm trigger:*
- JPEG mode: record 1 frame per second.
- H.264 mode: record I frame only.
- MPEG-4 mode: record the I frame only.

► *When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.*

The alarm trigger includes: motion detection and DI detection. Please refer to Event Settings on page 97.

■ Pre-event recording and post-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before and after a trigger is activated.

■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

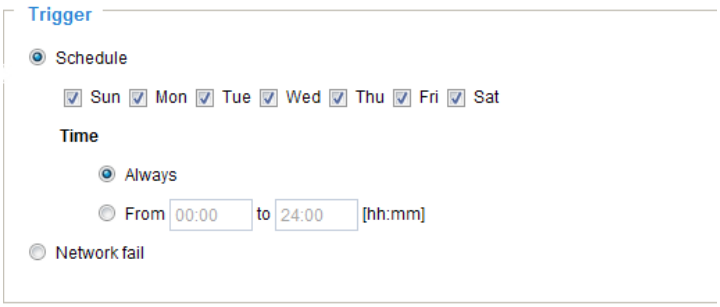
■ Source: Select a stream for the recording source.

NOTE:

► *To enable recording notification please configure **Event settings** first . Please refer to page 97.*

Please follow the steps below to set up the recording.

1. Trigger
Select a trigger source.



■ Schedule: The server will start to record files on the local storage or network storage (NAS).

■ Network fail: Since network fail, the server will start to record files on the local storage (SD card).

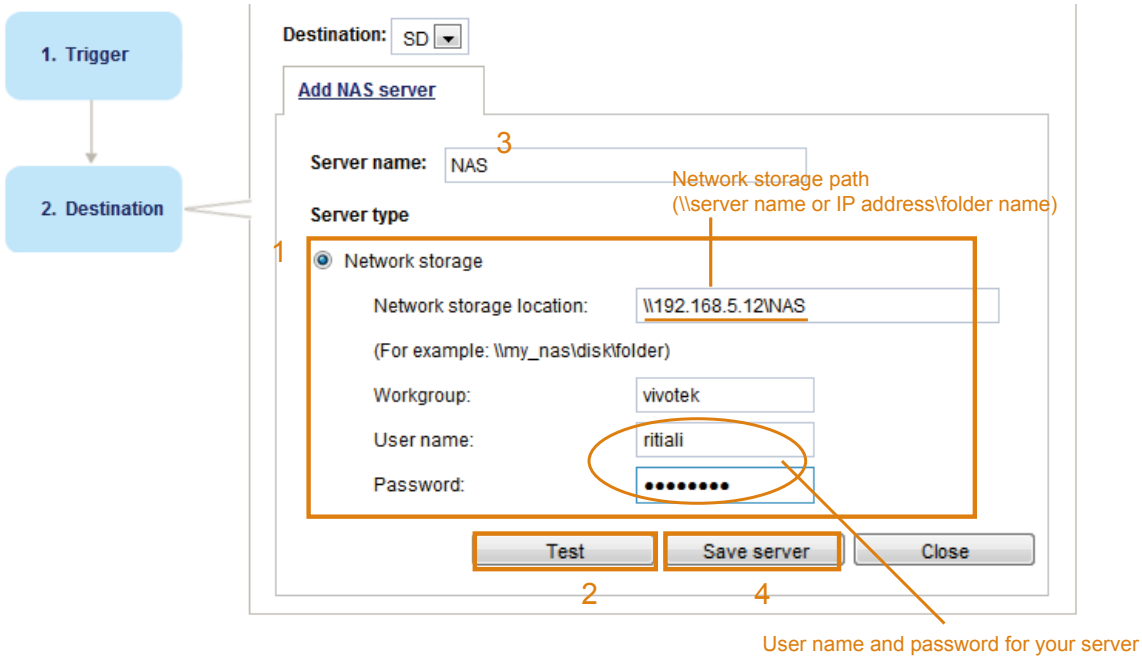
2. Destination

You can select the SD card or network storage (NAS) for the recorded video files.

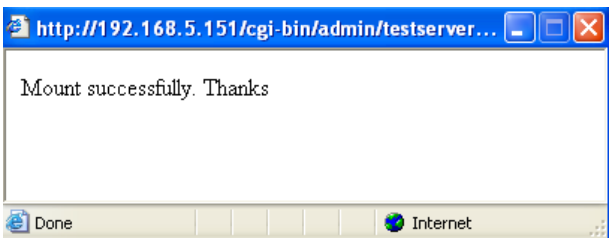
NAS server

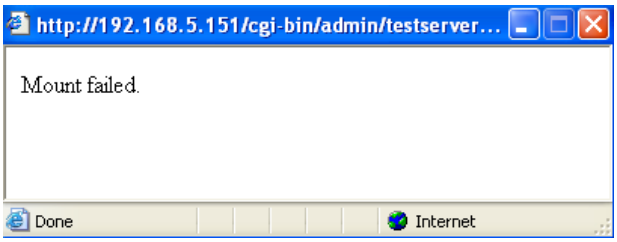
Click **Add NAS server** to open the server setting window and follow the steps below to set up:

1. Fill in the information for your server.
   For example:

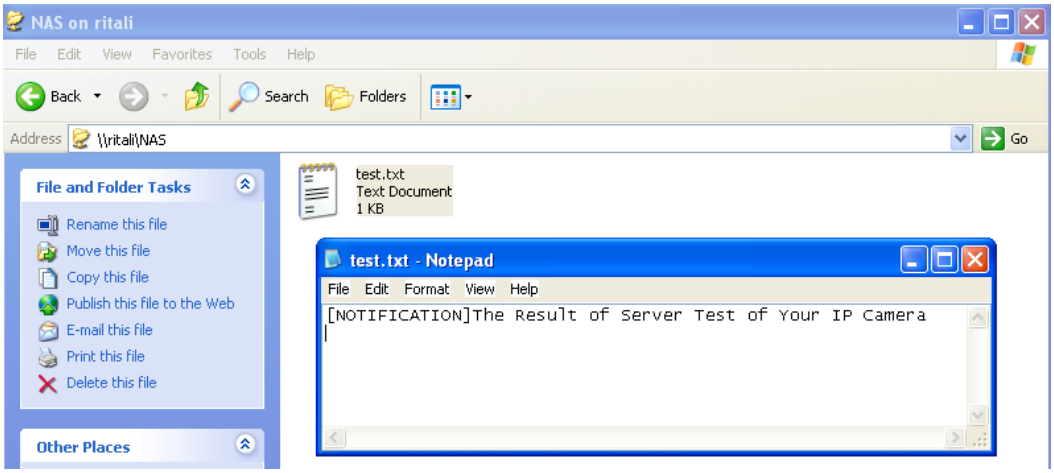


2. Click **Test** to check the setting. The result will be shown in the pop-up window.

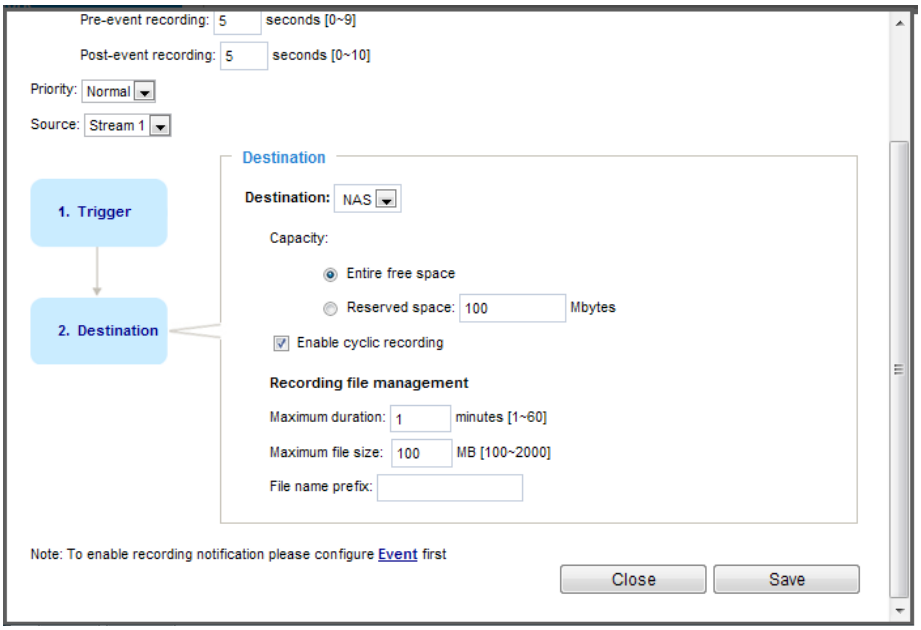




If successful, you will receive a test.txt file on the network storage server.



3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.



■ Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

■ Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for the transaction stage when the storage space is about to be full and new data arrives. The minimum for the Reserved space must be larger than 15 MBytes.

■ Maximum duraction: Specify the length of an individual video clip.

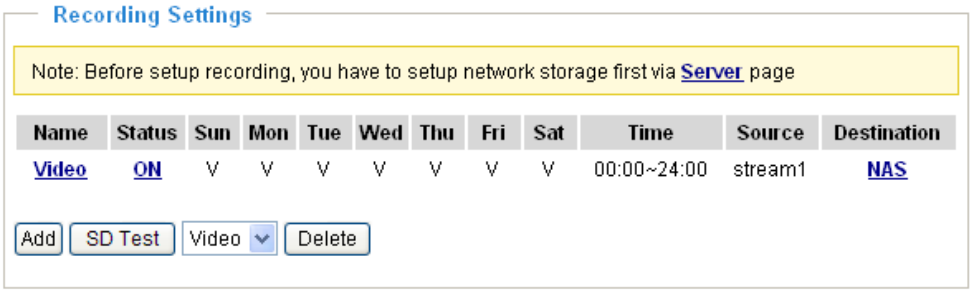
■ Maximum file size: Specify the file size of an individual clip.

■ File name prefix: Enter the text that will be appended to the front of the file name.

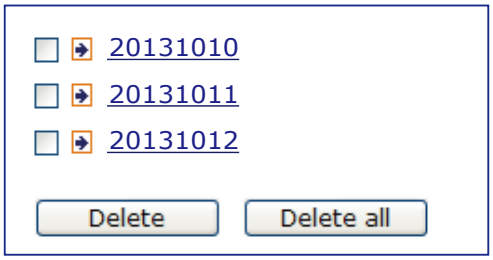
If you want to enable recording notification, please click ***Event*** to configure event triggering settings. Please refer to **Event > Event settings** on page 97 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage. The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.



- Click **Video (Name)**: Opens the Recording Settings page to modify.
- Click **ON (Status)**: The Status will become **OFF** and stop recording.
- Click **NAS (Destination)**: Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 122 for details.

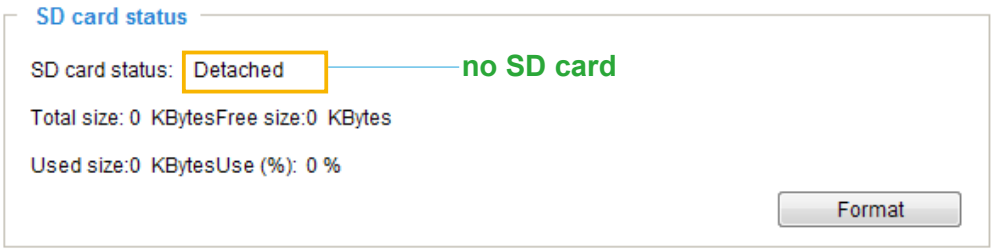


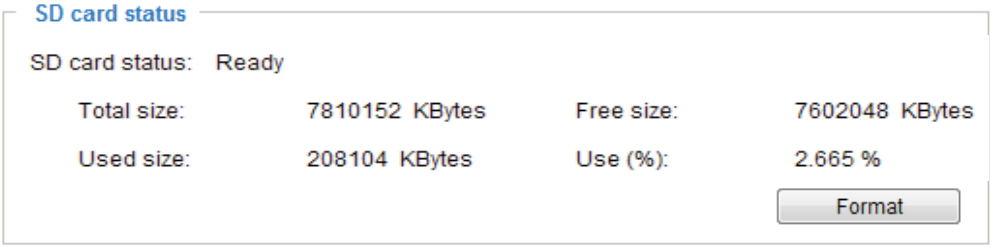
Local storage > SD card management Advanced Mode

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

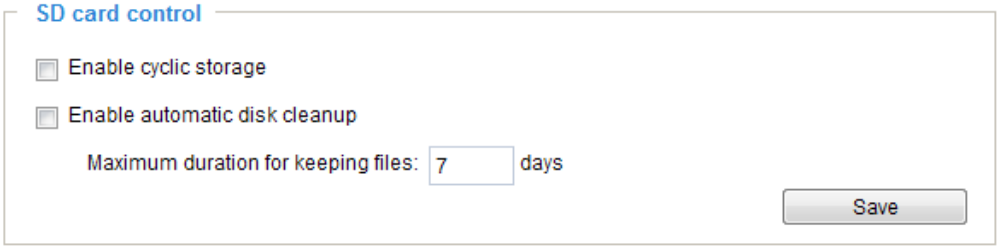
SD card staus

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.





SD card control



- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days. Files older than 7 days will automatically be cleaned up.

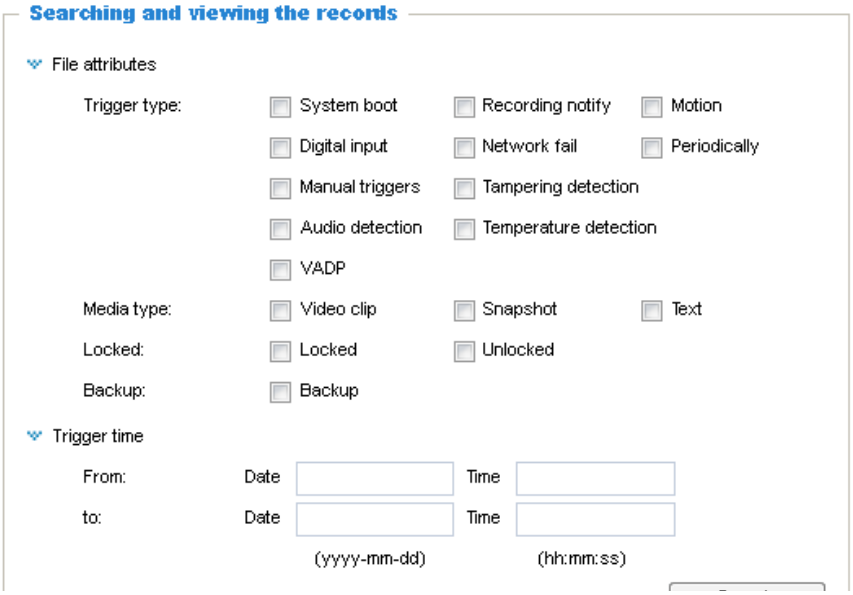
Click **Save** to enable your settings.

Local storage > Content management Advanced Mode

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** column.

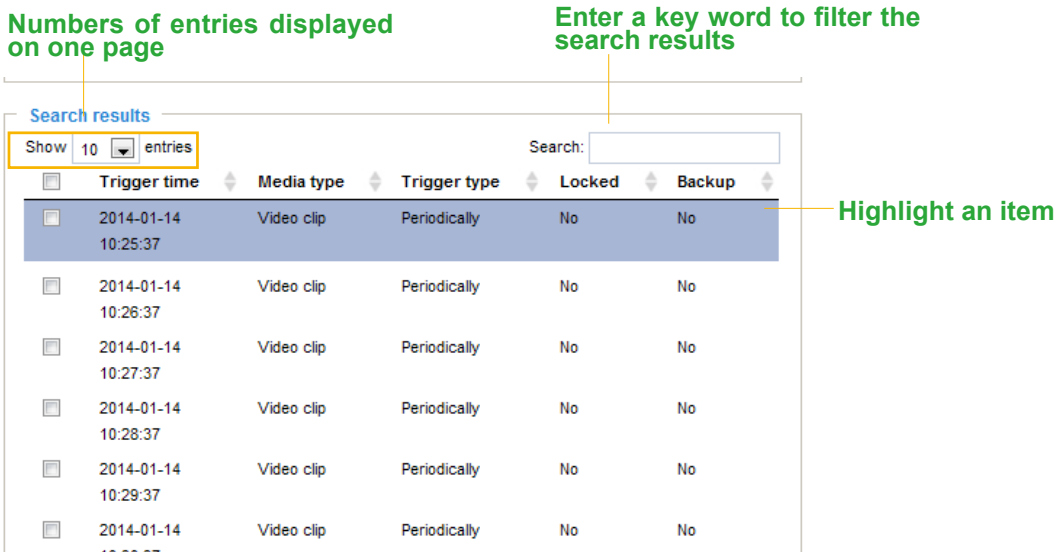


■ File attributes: Select one or more items as your search criteria.
■ Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⇕ to sort the search results in either direction.

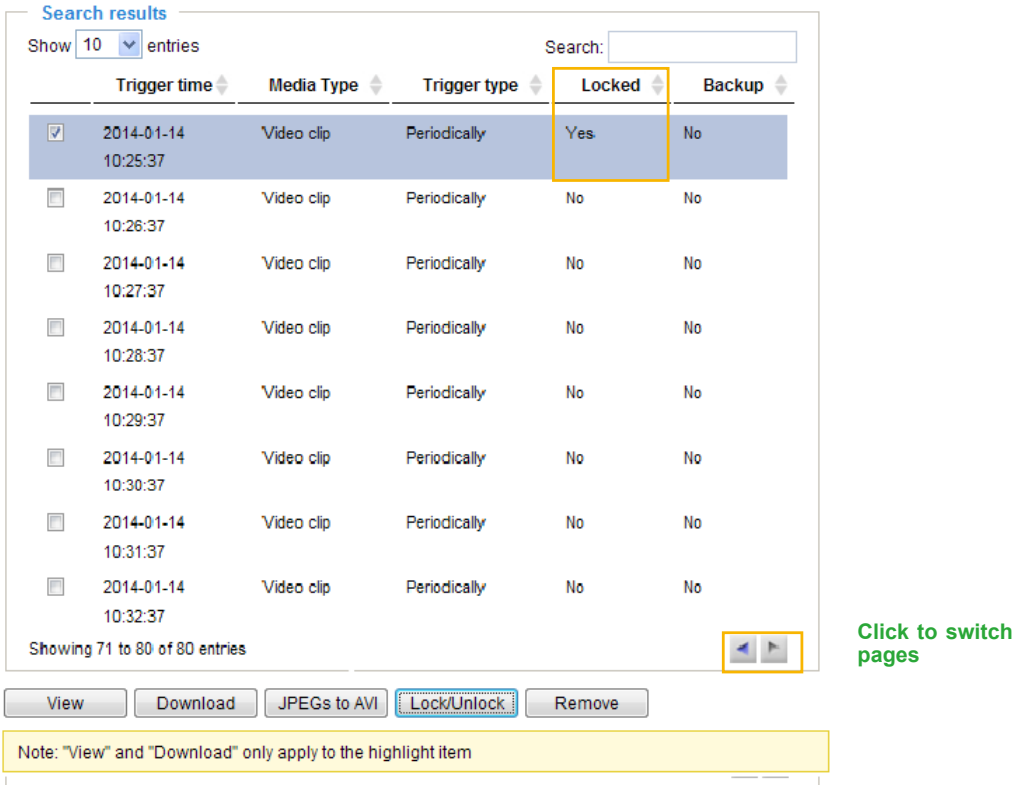


■ View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file. For example:

■ Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

■ JPEGs to AVI: This functions only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

■ Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections. For example:



Click to switch pages

■ Remove: Select the desired search results, then click this button to delete the files.

Appendix

URL Commands for the Network Camera

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

4. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

5. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]

[&<parameter>…]

http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]

Where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.
A successful control request returns parameter pairs as follows:
Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

6. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>.
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

7. Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters ",', <,>,& are invalid.
string[n~m]	Text strings longer than `n' characters and shorter than `m' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but displays '*' instead.
integer	Any number between (-2^{31} – 1) and (2^{31} – 1).
positive integer	Any number between 0 and (2^{32} – 1).
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description

integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

7.1 system

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[64]	Mega-Pixel Network Camera	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
lowlight	<boolean>	1	6/6	Turn on white light LED under all conditions. Only turn on white light LED in low light conditions.
date	<YYYY/MM/DD>, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	<blank>	6/6	Another current time format of the system.
ntp	<domain	<blank>	6/6	NTP server.

	name>, <ip address>, <blank>			*Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest,

				Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time

				in time zone.
daylight_dstactualmode	<boolean>	1~4	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time.
daylight_timezones	string	,-360,-320, -280,-240, -241,-200, -201,-160, -140,-120, -80,-40,0, 40,41,80, 81,82,83, 120,140, 380,400,48 0	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	99/6	Restore the system parameters to default values after <value> seconds.
reset	-1, 0, <positive integer>	N/A	99/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	0, <positive integer>	N/A	99/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	0,	N/A	99/6	Restore the system parameters to

	<positive integer>			default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	0, <positive integer>	N/A	99/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

7.1.1 system.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	MD8531H	0/99	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	MD8531H	0/99	ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	<product mac address>	0/99	12 characters MAC address (without hyphens).
firmwareversion	string[40]	<product dependent>	0/99	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/99	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	<product dependent>	0/99	Available language lists.

customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	<blank>	0/6	Custom language name.

7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	0	1/99	0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0)
do_i<0~(ndo-1)>	<boolean>	0	1/99	0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0)
daynight	day, night	<product dependent>	7/7	Current status of day, night.
onlinenum_rtsp	integer	0	0/0	Current number of RTSP connections.
onlinenum_httppush	integer	0	0/0	Current number of HTTP push server connections.
eth_i0	<string>	<product dependent>	1/99	Get network information from mii-tool.
vi_i<0~(nvi-1)>	<boolean>	0	1/99	Virtual input 0 => Inactive 1 => Active (capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	Indicates open circuit or closed circuit (inactive status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	open	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 security

Group: security

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_do <product dependent>	view, operator, admin	operator	1/6	Indicate which privileges and above can control digital output (capability.ndo > 0)
privilege_camctrl <product dependent>	view, operator, admin	view	1/6	Indicate which privileges and above can control PTZ (capability.ptzenabled > 0 or capability.eptz > 0)
user_i0_name	string[64]	root	6/7	User name of root
user_i<1~20>_name	string[64]	<blank>	6/7	User name
user_i0_pass	password[64]	<blank>	6/6	Root password
user_i<1~20>_pass	password[64]	<blank>	7/6	User password
user_i0_privilege	view, operator, admin	admin	6/7	Root privilege
user_i<1~20>_ privilege	view, operator, admin	<blank>	6/6	User privilege

7.6 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	<blank>	6/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=5556& network_rtp_videoport=20480"
type	lan, pppoe <product dependent>	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	<product dependent>	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.

dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	eap-peap	6/6	Selected EAP method
identity_peap	string[64]	<blank>	6/6	PEAP identity
identity_tls	string[64]	<blank>	6/6	TLS identity
password	string[253]	<blank>	6/6	Password for TLS
privatekeypassword	string[253]	<blank>	6/6	Password for PEAP
ca_exist	<boolean>	0	6/6	CA installed flag
ca_time	<integer>	0	6/7	CA installed time. Represented in EPOCH
ca_size	<integer>	0	6/7	CA file size (in bytes)
certificate_exist	<boolean>	0	6/6	Certificate installed flag (for TLS)
certificate_time	<integer>	0	6/7	Certificate installed time. Represented in EPOCH
certificate_size	<integer>	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	0	6/6	Private key installed flag (for TLS)
privatekey_time	<integer>	0	6/7	Private key installed time. Represented in EPOCH
privatekey_size	<integer>	0	6/7	Private key file size (in bytes)

7.6.2 QOS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	1	6/6	VLAN ID
video	0~7	0	6/6	Video channel for CoS
audio	0~7	0	6/6	Audio channel for CoS (capability.naudio > 0)
eventalarm	0~7	0	6/6	Event/alarm channel for CoS
management	0~7	0	6/6	Management channel for CoS
eventtunnel	0~7	0	6/6	Event/Control channel for CoS

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable DSCP
video	0~63	0	6/6	Video channel for DSCP
audio	0~63	0	6/6	Audio channel for DSCP (capability.naudio > 0)
eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
management	0~63	0	6/6	Management channel for DSCP
eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address>	<blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address>	<blank>	6/6	IPv6 router address.
addondns	<ip address>	<blank>	6/6	IPv6 DNS address.
allowoptional	<boolean>	0	6/6	Allow manually setup of IP address setting.

7.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	21	6/6	Local ftp server port.

7.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	1/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
s0_accessname	string[32]	video.mjpg	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)
s1_accessname	string[32]	video2.mjpg	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)
s2_accessname	string[32]	video3.mjpg	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2)
S3_accessname	string[32]	Vide04.mjpg	1/6	Http server push access name for anystream. (capability.protocol.spush.mjpeg = 1 and capability.nanystream = 1)
anonymousviewing	<boolean>	0	1/6	Enable anonymous streaming viewing.

7.6.6 HTTPS port

Subgroup of **network**: **https_port** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	443	1/6	HTTPS port.

7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and capability.nmediastream > 0)
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and capability.nmediastream > 1)
s2_accessname	string[32]	live3.sdp	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and capability.nmediastream > 2)
s3_accessname	string[32]	Live4.sdp	1/6	RTSP access name for stream4. (capability.protocol.rtsp=1 and capability.nmediastream > 3)

7.6.7.1 RTSP multicast

Subgroup of **network_rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	0	4/4	Enable always multicast.
ipaddress	<ip address>	For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on.	4/4	Multicast IP address.
videoport	1025 ~ 65535	5562+n*6	4/4	Multicast video port.
audioport	1025 ~ 65535	5564+n*6	4/4	Multicast audio port. (capability.naudio > 0)
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	1/6	SIP port.

7.6.9 RTP port

Subgroup of **network**: **rtp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

7.6.10 PPPoE

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user	string[128]	<blank>	6/6	PPPoE account user name.
pass	password[64]	<blank>	6/6	PPPoE account password.

7.7 IP Filter

Group: ipfilter

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	string[43]	<blank>	6/6	Administrator IP address.
maxconnection	0~10	10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address> Network address: <ip address / network mask> Range address:<start ip address - end ip address>	<blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	string[43]	<blank>	6/6	IPv6 address list.

7.8 Video input

Group: **videoin**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	1/4	CMOS frequency. (capability.videoin.type=2)
whitebalance	auto, auto2, manual, manual2, rbgain	auto	1/4	"auto" indicates auto white balance. "auto2" indicates auto white balance 2 which is designed for non-bundle lens models. "manual" indicates keep current value. "manual2" indicates keep current value for auto2. "rbgain" indicates using rgain and gbain.
exposurelevel	0~12	6	1/4	Exposure level
autoiris	<boolean>	0	1/4	Enable auto Iris.
irismode	fixed, indoor, outdoor	fixed	1/4	Video Iris for DC Iris.
enablewdr	<boolean>	0	1/4	Enable/disable wield dynamic range.
enableblc	<boolean>	0	1/4	Enable backlight compensation.
agc	0,1,2	1	1/4	Set auto gain control to normal level or MAX level. 0->2x, 1->4x, 2->8x
color	0, 1	1	1/4	0 =>monochrome 1 => color
flip	<boolean>	0	1/4	Flip the image.
mirror	<boolean>	0	1/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support)

				Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[64]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	1/4	Overlay time stamp on video.
maxexposure	1, 15, 30, 60, 120, 240, 480	30	1/4	Maximum exposure time.
enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.
rotate	0, 90, 270	0	4/4	0=> rotation off 90=> rotate 90 degrees clockwise 270=> rotate 270 degrees clockwise

7.8.1 Video input setting per channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	1/4	CMOS frequency. (capability.videoin.type=2)
mode	0 ~ "capability_videoin_c<n>_nmode"-1	0	1/4	Set video mode.
whitebalance	auto, manual, rbgain	auto	1/4	"auto" indicates auto white balance. "manual" indicates keep current value. "rbgain" indicates using rgain and gbain.
rgain	0~100	30	1/4	Manual set rgain value of gain

				control setting.
bgain	0~100	30	1/4	Manual set bgain value of gain control setting.
exposurelevel	0~12	6	1/4	Exposure level
autoiris	0~1	0	1/4	set 1 to enable auto iris, set 0 to disable auto iris.
irismode	fixed	fixed	1/4	Video Iris for DC Iris.
enableblc	0~1	0	1/4	Enable backlight compensation
agc	0,1,2	1	1/4	Set auto gain control to normal level or MAX level. 0->2x, 1->4x, 2->8x
agcmode	auto,fixed	auto	1/4	Set auto gain control mode.
maxgain	0~100	100	1/4	Manual set maximum gain value.
mingain	0~100	0	1/4	Manual set minimum gain value.
color	0, 1	1	1/4	0 =>monochrome 1 => color
flip	<boolean>	0	1/4	Flip the image.
mirror	<boolean>	0	1/4	Mirror the image.
text	string[64]	<blank>	1/4	Enclose caption.
textonvideo_position	top, bottom	top	1/4	Position of timestamp and video title on image
textonvideo_size	15,25,30	15	1/4	Timestamp and video title font-size
imprinttimestamp	<boolean>	0	1/4	Overlay time stamp on video.
exposuremode	auto,fixed	auto	1/4	Exposure mode
minexposure	1~32000	32000	1/4	Minimum exposure time.
maxexposure	1~32000	30	1/4	Maximum exposure time.
enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.
crop_position	<coordinate> (x,y)	0,0	1/99	Crop left-top corner coordinate.
crop_size	<window size>	1280x960	1/99	Crop width and height.

	(WxH)			(width must be 16x or 32x and height must be 8x)
crop_preview	< boolean >	0	1/99	Usage for UI of crop setting
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	h264	1/4	Video codec type.
s<0~(m-1)>_resolution	Reference capability_videoin_resolution	1280x960 (2nd stream: 800x600; 3rd stream: 640x480)	1/4	Video resolution in pixels.
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	1/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	cbr	1/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_prioritypolicy	framerate, imagequality	framerate (3nd stream: Imagequality 4th stream: imagequality)	1/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_mpeg4_quant	1~5, 99, 100	3	1/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mpeg4_qvalue	2~31	7	1/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 99)
s<0~(m-1)>_mpeg4_qpercent	1~100	50	1/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant =

				100)
s<0~(m-1)>_mpeg4_bitrate	4000~40000000	3000000 (3rd stream: 512000)	1/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mpeg4_maxvbrbitrate	1000~"capability_videoin_c<n>_mpeg4_maxbitrate"	40000000	1/4	The maximum allowed bit rate in fixed quality mode. When the bit rate exceeds this value, frames will be dropped to restrict the bit rate. * Only valid when "ratecontrolmode"= vbr
s<0~(m-1)>_mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	30 (3rd stream: 15)	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	1/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	cbr	1/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_prioritypolicy	framerate, imagequality	framerate	1/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_h264_quant	1~5, 99, 100	3	1/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_h264_qvalue	0~51	29	1/4	Manual video quality level input.

				(s<0~(m-1)>_h264_quant = 99)
s<0~(m-1)>_h264_qpercent	1~100	50	1/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_bitrate	4000~40000000	3000000 (3rd stream: 512000)	1/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_h264_maxvbrbitrate	1000~"capability_videoin_c<n>_h264_maxbitrate"	40000000	1/4	The maximum allowed bit rate in fixed quality mode. When the bit rate exceeds this value, frames will be dropped to restrict the bit rate. * Only valid when "ratecontrolmode"= vbr
s<0~(m-1)>_h264_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	30	1/4	Set maximum frame rate in fps (for h264).
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_ mjpeg _ratecontrolmode	cbr, vbr	vbr	1/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mjpeg_prioritypolicy	framerate, imagequality	framerate (3rd stream: imagequality 4th stream: imagequality)	1/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_mjpeg_quant	1~5, 99, 100	3	1/4	Quality of JPEG video. 99 is the customized manual input setting.

				1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mjpeg_qvalue	2~97	29	1/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 99)
s<0~(m-1)>_mjpeg_qpercent	1~100	50	1/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 100)
s<0~(m-1)>_mjpeg_bitrate	1000~40000000	14000000	1/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mjpeg_maxvbrbitrate	4000~"capability_videoin_c<n>_mjpeg_maxbitrate"	60000000 (3rd stream: 512000)	1/4	The maximum allowed bit rate in fixed quality mode. When the bit rate exceeds this value, frames will be dropped to restrict the bit rate. * Only valid when "ratecontrolmode"= vbr
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	30	1/4	Set maximum frame rate in fps (for JPEG).
wdr_mode	0~1	1	1/4	Turning WDR Pro on or off. 0: off 1: on
wdr_strength	0~2	1	1/4	The strength of WDR Pro. 0: low 1: medium 2: high
wdr_sensitivity	1~100	50	1/4	The sensitivity of WDR Pro. 1~33: low 34~67: medium 68~100: high
aespeed_mode	0~1	0	1/4	Turning AE converge speed on or off. 0: off 1: on
aespeed_speedlevel	1~100	60	1/4	The speed level of AE converge

				speed. 1~20: level 1 21~40: level 2 41~60: level 3 61~80: level 4 81~100: level 5
aespeed_sensitivity	1~100	60	1/4	The sensitivity of AE converge speed. 1~20: level 1 21~40: level 2 41~60: level 3 61~80: level 4 81~100: level 5
flickerless	0~1	0	1/4	Turn on(1) or turn off(0) the flickerless mode

7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: **videoin_c0_profile_i<0~(m-1)>** (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	1/4	Enable/disable this profile setting
policy	day, night, schedule	night	1/4	The mode which the profile is applied to.
begintime	hh:mm	18:00	1/4	Begin time of schedule mode.
endtime	hh:mm	06:00	1/4	End time of schedule mode.
exposuremode	auto,fixed	auto	1/4	Exposure Mode
minexposure	1~32000	32000	1/4	Minimum exposure time.
maxexposure	1~32000	30	1/4	Maximum exposure time.
enableblc	<boolean>	0	1/4	Enable backlight compensation.
exposurelevel	0~12	6	1/4	Exposure level
agc	0,1,2	2	1/4	Set auto gain control to normal level or MAX level. 0->2x, 1->4x, 2->8x

agcmode	auto,fixed	auto	1/4	Set auto gain control mode.
maxgain	0~100	100	1/4	Manual set maximum gain value.
mingain	0~100	0	1/4	Manual set minimum gain value.
autoiris	<boolean>	0	1/4	Enable auto Iris.
whitebalance	auto, manual, rbgain	auto	1/4	"auto" indicates auto white balance. "manual" indicates keep current value. "rbgain" indicates using rgain and gbain.
rgain	0~100	30	1/4	Manual set rgain value of gain control setting.
bgain	0~100	30	1/4	Manual set bgain value of gain control setting.
irismode	fixed, indoor, outdoor	fixed	1/4	Video Iris for DC Iris.
wdr_mode	0~1	1	1/4	Turning WDR Pro on or off. 0: off 1: on
wdr_strength	0~2	1	1/4	The strength of WDR Pro. 0: low 1: medium 2: high
wdr_sensitivity	1~100	50	4/4	The sensitivity of WDR Pro. 1~33: low 34~67: medium 68~100: high
flickerless	0~1	0	1/4	Turn on(1) or turn off(0) the flickerless mode
aespeed_mode	0~1	0	1/4	Turning AE converge speed on or off. 0: off 1: on
aespeed_speedlevel	1~100	60	1/4	The speed level of AE converge speed. 1~20: level 1 21~40: level 2 41~60: level 3 61~80: level 4 81~100: level 5

aespeed_sensitivity	1~100	60	1/4	The sensitivity of AE converge speed. 1~20: level 1 21~40: level 2 41~60: level 3 61~80: level 4 81~100: level 5

7.9 Video input preview

The temporary settings for video preview

Group: videoinpreview

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
exposuremode	auto,fixed	auto	4/4	Exposure Mode
minexposure	1~32000	32000	4/4	Minimum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
exposurelevel	0~12	6	4/4	Exposure level
enableblc	<boolean>	0	4/4	Enable backlight compensation.
irismode	Fixed, indoor, outdoor	fixed	4/4	Video Iris for DC Iris.
wdr_mode	0~1	1	4/4	Turning WDR Pro on or off. 0: off 1: on
wdr_strength	0~2	1	4/4	The strength of WDR Pro. 0: low 1: medium 2: high
wdr_sensitivity	1~100	50	4/4	The sensitivity of WDR Pro. 1~33: low 34~67: medium 68~100: high
agc	0,1,2	1	4/4	Set auto gain control to normal level or MAX level. 0->2x, 1->4x, 2->8x
agcmode	auto,fixed	auto	4/4	Set auto gain control mode.
maxgain	0~100	100	4/4	Manual set maximum gain value.

mingain	0~100	0	4/4	Manual set minimum gain value.
autoiris	<boolean>	0	4/4	Enable auto Iris.
aespeed_mode	0~1	0	4/4	Turning AE converge speed on or off. 0: off 1: on
aespeed_speedlevel	1~100	60	4/4	The speed level of AE converge speed. 1~20: level 1 21~40: level 2 41~60: level 3 61~80: level 4 81~100: level 5
aespeed_sensitivity	1~100	60	4/4	The speed level of AE converge speed. 1~20: level 1 21~40: level 2 41~60: level 3 61~80: level 4 81~100: level 5

7.10 Image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	-5	4/4	Adjust brightness of image according to mode settings.
saturation	-5~5,100	0	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation=100
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
sharpness	-3~3,100	0	4/4	Adjust sharpness of image according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of

				percentage when sharpness=100
gammacurve	0~100	0	4/4	Gamma curve.
lowlightmode	<boolean>	1	4/4	Enable/disable low light mode.
dnr_mode	0~1	0	4/4	Enable/disable noise reduction
dnr_strength	1~100	50	4/4	The strength of noise reduction. 1~33: low 34~67: medium 68~100: high
profile_i0_enable	<boolean>	0	4/4	Enable/disable this profile setting
profile_i0_policy	day, night, schedule	schedule	4/4	The mode which the profile is applied to.
profile_i0_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
profile_i0_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i0_brightness	-5~5	-5	4/4	Adjust brightness of image according to mode settings.
profile_i0_contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
profile_i0_saturation	-5~5,100	0	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
profile_i0_saturationpercent	0~100	50	4/4	when profile_i0_saturation=100, adjust saturation value of percentage according to mode settings.
profile_i0_sharpness	-3~3,100	0	4/4	Adjust sharpness of image according to mode settings.
profile_i0_sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100
profile_i0_gammacurve	0~100	0	4/4	Gamma curve
profile_i0_lowlightmode	<boolean>	1	4/4	Enable/disable low light mode.
profile_i0_dnr_mode	0~1	0	4/4	Enable/disable noise reduction
profile_i0_dnr_strength	1~100	50	4/4	The strength of noise reduction. 1~33: low 34~67: medium 68~100: high

7.11 Image setting for preview

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	-5	4/4	Adjust brightness of image according to mode settings.
saturation	-5~5,100	0	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation=100
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
sharpness	-3~3,100	0	4/4	Adjust sharpness of image according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100
gammacurve	0~100	0	4/4	Gamma curve
lowlightmode	<boolean>	1	4/4	Enable/disable low light mode.
dnr_mode	0~1	0	4/4	Enable/disable noise reduction
dnr_strength	1~100	50	4/4	The strength of noise reduction. 1~33: low 34~67: medium 68~100: high

Group: imagepreview

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoin_whitebalance	auto, manual, rbgain	auto	4/4	"auto" indicates auto white balance. "manual" indicates keep current value. "rbgain" indicates using rgain and gbain.
videoin_restoreatwb	0, 1~	0	4/4	Restore of adjusting white balance of image according to mode settings
videoin_rgain	0~100	0	4/4	Manual set rgain value of gain control setting.

videoin_bgain	0~100	0	4/4	Manual set bgain value of gain control setting.

7.12 Audio input per channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
source	linein, micin	micin	4/4	micin => use built-in microphone input.
mute	0, 1	0	1/4	Disable audio mute.
gain	0~100	65	4/4	Gain of input (%). (audioin_c<0~(n-1)>_source = linein)
boostmic	0~100	65	4/4	Enable microphone boost. 0 => +0dB 1 => +20dB 2 => +40dB Or Gain of input (%). (audioin_c<0~(n-1)>_source = micin)
s<0~(m-1)>_codectype	g711, g726	g711	4/4	Set audio codec type for input.
s<0~(m-1)>_g726_bitrate <product dependent>	16000, 24000, 32000, 40000	32000	4/4	Set G.726 bitrate in bps.
s<0~(m-1)>_g711_mode <product dependent>	pcmu, pcma	pcmu	4/4	Set G.711 mode.

7.13 Motion detection settings

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[40]	<blank>	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

Group: **motion_c<0~(n-1)> profile** for m profile and n channel product (capability.nmotionprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
i<0~(m-1)>_enable	<boolean>	0	4/4	Enable profile 1 ~ (m-1).
i<0~(m-1)>_policy	day, night, schedule	night	4/4	The mode which the profile is applied to.
i<0~(m-1)>_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
i<0~(m-1)>_endtime	hh:mm	06:00	4/4	End time of schedule mode.
i<0~(m-1)>_win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window.
i<0~(m-1)>_win_i<0~2>_name	string[40]	<blank>	4/4	Name of motion window.
i<0~(m-1)>_win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
i<0~(m-1)>_win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
i<0~(m-1)>_win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion

				detection window.
i<0~(m-1)>_win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
i<0~(m-1)>_win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
i<0~(m-1)>_win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

7.14 Tempering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (capability.tampering > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	1/7	Threshold of tamper detection.
duration	10 ~ 600	10	4/4	If tampering value exceeds the 'threshold' for more than 'duration' second(s), then tamper detection is triggered.

7.15 DDNS

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	Safe100, PeanutHull, DyndnsDynamic, DyndnsCustom, DynInterfree, CustomSafe100	DyndnsDynamic	6/6	Safe100 => safe100.net PeanutHull => PeanutHull DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) DynInterfree =>dyn-interfree.it CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.

<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

7.16 Express link

Group: expresslink

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable express link.
state	onlycheck, onlyoffline, checkonline, badnetwork	badnetwork	6/6	Camera will check the status of network environment and express link URL
url	string[63]	NULL	6/6	The url user define to link to camera

7.17 UPnP presentation

Group: upnppresentation

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	1	6/6	Enable or disable the UPnP presentation service.

7.18 UPnP port forwarding

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPnP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

7.19 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG
setparamlevel	0~2	0	6/6	Show log of parameter setting. 0: disable 1: Show log of parameter setting set from external. 2. Show log of parameter setting set from external and internal.

7.20 UART control

Group: **uart** (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	<blank>	1/4	Name of the PTZ driver.
ptzdrivers_i<0~19, 127>_location	string[128]	<blank>	1/4	Full path of the PTZ driver.
enablehttptunnel	<boolean>	0	1/4	Enable HTTP tunnel channel to control UART.

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	9600	4/4	Set baud rate of COM port.
databit	5,6,7,8	8	4/4	Data bits in a character frame.
paritybit	none, odd, even	none	4/4	For error checking.
stopbit	1,2	1	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	rs485	4/4	RS485 or RS232.
customdrvcmd_i<0~9>	string[128]	<blank>	1/4	PTZ command for custom camera.
speedlink_i<0~4>_name	string[40]	<blank>	1/4	Additional PTZ command name.
speedlink_i<0~4>_cmd	string[40]	<blank>	1/4	Additional PTZ command list.
ptzdriver	0~19, 127 (custom), 128 (no driver)	128 (no driver)	1/4	The PTZ driver is used by this COM port.

7.21 SNMP

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name
authpwrw	string[8~128]	<blank>	6/6	Read/write authentication password

authpwro	string[8~128]	<blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank>	6/6	Read/write passwrd
encryptpwro	string[8~128]	<blank>	6/6	Read only password
encrypttyperw	DES	DES	6/6	Read/write encryption type
encrypttypero	DES	DES	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Read only community
syslocation	string[128]	<blank>	6/6	System location
syscontact	string[128]	<blank>	6/6	System contact

7.22 Layout configuration

Group: **layout** (New version)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[64]	http://www.vivotek.com	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
custombutton_manualtrigger_show	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.

theme_color_controlbackground	string[7]	#565656	1/6	Background color of control area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color

7.23 Privacy mask

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean>	0	4/4	Enable privacy mask window.
win_i<0~4>_name	string[40]	<blank>	4/4	Name of the privacy mask window.
win_i<0~4>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 320	0	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320	0	4/4	Width of privacy mask window.
win_i<0~4>_height	0 ~ 320	0	4/4	Height of privacy mask window.

7.24 Capability

Group: capability

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string>	0300a	0/99	The HTTP API version.
bootuptime	<positive integer>	60	0/99	Server bootup time.
nir	0, <positive integer>	0	0/99	Number of IR interfaces. (Recommand to use ir for built-in IR and extir for external IR)
npir	0, <positive integer>	0	0/99	Number of PIRs.

ndi	0, <positive integer>	1	0/99	Number of digital inputs.
nvi	0, <positive integer>	3	0/99	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	1	0/99	Number of digital outputs.
naudioin	0, <positive integer>	1	0/99	Number of audio inputs.
naudioout	0, <positive integer>	1	0/99	Number of audio outputs.
nvideoin	<positive integer>	1	0/99	Number of video inputs.
nmediastream	<positive integer>	4	0/99	Number of media stream per channels.
nvideosetting	<positive integer>	4	0/99	Number of video settings per channel.
naudiosetting	<positive integer>	1	0/99	Number of audio settings per channel.
nuart	0, <positive integer>	0	0/99	Number of UART interfaces.
nvideoinprofile	<positive integer>	1	0/99	Number of video input profiles.
nmotion	0, <positive integer>	3	0/99	Number of motion window.
nmotionprofile	0, <positive integer>	1	0/99	Number of motion profiles.
ptzenabled	0, <positive integer>	0	0/99	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in)

				Bit 2 => Support pan operation, 0(not support), 1(support) Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support), 1(support) Bit 6 => Support iris operation; 0(not support), 1(support) Bit 7 => External or built-in PT; 0(built-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
evctrlchannel	<boolean>	1	0/99	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	1	0/99	Indicate whether to support joystick control.
storage_dbenabled	<boolean>	1	0/99	Media files are indexed in database.
ptzenabledclient	<boolean>	0	0/99	Indicate whether to support ptz client
protocol_https	< boolean >	1	0/99	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/99	Indicate whether to support RTSP.
protocol_sip	<boolean>	1	0/99	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/99	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/99	The maximum general streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/99	The maximum megapixel streaming connections.
protocol_rtp_multicast_ scalable	<boolean>	1	0/99	Indicate whether to support scalable multicast.

protocol_rtp_multicast_ backchannel	<boolean>	0	0/99	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/99	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/99	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	1	0/99	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/99	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/99	Indicate whether to support IPv6.
videoin_type	0, 1, 2	2	0/99	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_codec	mpeg4. mjpeg, h264	mpeg4, mjpeg, h264	0/99	Available codec of a device. The sequence is not limited. EX: IP7361 supports MPEG4 and MJPEG, then this is "mpeg4,mjpeg". IP8371E supports MPEG4, MJPEG and H.264, then this is "mpeg4,mjpeg,h264"
videoin_streamcodec	<Positive Integer>	7,7,7	0/99	This equals "capability_videoin_c0_streamcodec".
videoin_flexiblebitrate	0, 1	1	0/99	Support flexible bit rate control or not.
videoin_resolution	<a list of available resolution separated by commas>	176x144, 320x240, 640x480, 800x600, 1280x960	0/99	Available resolutions list.
videoin_nresolution	< number of available resolution list>	5	0/99	How many resolution options (listed in "resolution") in current video mode.
videoin_maxframerate	<a list of available	30, 30,	0/99	Available maximum frame list.

	maximum frame rate separated by commas>	30, 30, 30		
videoin_mpeg4_maxframerate	<a list of available maximum codec frame rate separated by commas>	30, 30, 30, 30, 30	0/99	Available maximum codec frame list.
videoin_mjpeg_maxframerate	<a list of available maximum codec frame rate separated by commas>	30, 30, 30, 30, 30	0/99	Available maximum codec frame list.
videoin_h264_maxframerate	<a list of available maximum codec frame rate separated by commas>	30, 30, 30, 30, 30	0/99	Available maximum codec frame list.
videoout_codec	<a list of the available codec types separated by commas)	<blank>	0/99	Available codec list.
audio_aec	<boolean>	0	0/99	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0	0/99	Indicate whether to support external microphone input.

audio_linein	<boolean>	0	0/99	Indicate whether to support external line input. (It will be replaced by audio_mic and audio_extmic.)
audio_lineout	<boolean>	1	0/99	Indicate whether to support line output.
audio_headphoneout	<boolean>	0	0/99	Indicate whether to support headphone output.
audioin_codec	g711, g726 <product dependent>	g711, g726	0/99	Available codec list for audio input.
camctrl_httptunnel	<boolean>	0	0/99	Indicate whether to support httptunnel.
camctrl_httptunnelclient	<boolean>	0	0/99	Indicate whether to support httptunnel client.
camctrl_privilege	<boolean>	1	0/99	Indicate whether to support "Manage Privilege" of PTZ control in the Security page. 1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi
uart_httptunnel	<boolean>	0	0/99	Indicate whether to support HTTP tunnel for UART transfer.
transmission_mode	Tx, Rx, Both	Tx	0/99	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/99	Indicate whether to support Ethernet.
network_wireless	<boolean>	0	0/99	Indicate whether to support wireless.
derivative_brand	<boolean>	1	0/99	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
npreset	0, <positive integer>	20	0/99	Number of preset locations

eptz	0, <positive integer>	3	0/99	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
nanystream	0, <positive integer>	0	0/99	number of any media stream per channel
iva	<boolean>	0	0/99	Indicate whether to support Intelligent Video analysis
tampering	<boolean>	1	0/99	Indicate whether to support tampering detection.
test_ac	<boolean>	1	0/99	Indicate whether to support test ac key.
version_onvifdaemon	<string>	1.7.1.12	0/99	Indicate ONVIF daemon version
image_wdrc	<Boolean>	0	0/99	Indicate whether to support WDR enhanced.
image_ iristype	<string>	fixediris	0/99	Indicate iris type.
image_ focusassist	<Boolean>	0	0/99	Indicate whether to support focus assist.
adaptiverecording	<boolean>	1	0/99	Indicate whether to support adaptive recording.
adaptivestreaming	<boolean>	1	0/99	Indicate whether to support adaptive streaming.
temperature	<boolean>	1	0/99	Indicate whether to support temperature detection.

7.26 WebAPI: Information for a channel

Group: capability_videoin_c<n>, n = channel index from 0 to "capability_nvideoin"-1

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
nmode	<Positive Integer>	2	0/99	Indicate how many video modes supported by this channel.
maxsize	<WxH>	1280x960	0/99	The maximum resolution of all modes in this channel, the unit is pixel.
mode	<Integer>	0	0/99	Indicate current video mode.
nresolution	<Positive Integer>	5	0/99	How many resolution options (listed in "resolution") in current video mode.
resolution	A list of <WxH>	176x144, 320x240, 640x480, 800x600, 1280x960	0/99	Resolution options in current video mode. These options are the possible options for "videoin_c<n>_s<m>_resolution". The last one is the maximum resolution in current mode.
maxframerate	A list of <Integer>	30, 30, 30, 30, 30	0/99	Indicate how many frame rate image sensor outputs in current video mode. One to one mapping to the resolution in "resolution".
mpeg4_maxframerate	A list of <Integer> and "-"	30, 30, 30, 30, 30	0/99	Maximum fps that the device can encoded with MPEG4 on resolutions in current video mode. "-" means not support.
mpeg4_maxbitrate	<Positive Integer>	40000000	0/99	Maximum bitrates of MPEG4. The unit is bps.
mjpeg_ maxframerate	A list of <Positive Integer> and "-"	30, 30, 30, 30, 30	0/99	Maximum fps that the device can encoded with MJPEG on resolutions in current video mode. "-" means not support.

mjpeg_maxbitrate	<Positive Integer>, -	40000000	0/99	Maximum bitrates of MJPEG. The unit is bps. "-" means MJPEG does not support bit rate control.
h264_ maxframerate	A list of <Positive Integer> and "-"	30, 30, 30, 30, 30	0/99	Maximum fps that the device can encoded with H.264 on resolutions in current video mode. "-" means not support.
h264_maxbitrate	<Positive Integer>	40000000	0/99	Maximum bitrates of H.264. The unit is bps.
streamcodec	<Positive Integer>	7,7,7	0/99	Represent supported codec types of each stream. This contains a list of positive integers, split by comma. Each one stands for a stream, and the definition is as following: Bit 0: Support MPEG4. Bit 1: Support MJPEG Bit 2: Support H.264

7.27 WebAPI: Information for a mode

Group: capability_videoin_c<n>_mode<m>, n = channel index from 0 to "capability_nvideoin"-1, m = mode index from 0 to "capability_videoin_c<n>_nmode"-1

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
effectivepixel	<WxH>	<mode dependent>	0/99	The visible area of full scene in this video mode. The unit is pixel in source.
outputsize	<WxH>	<mode dependent>	0/99	The output size of source, equal to the captured size by device, in this video mode. The unit is pixel. This value is used as a basic coordinate system for many features, like ePTZ, privacy mask, motion, etc.

binning	0, 1, 3	<mode dependent>	0/99	Indicate binning is used or not in this video mode. 0: No binning 1: 2x2 binning 3: 3x3 binning
nresolution	<Positive Integer>	<mode dependent>	0/99	How many resolution options in this video mode.
resolution	A list of <WxH>	<mode dependent>	0/99	Resolution options in this video mode. The last one is the maximum resolution in this video mode.
maxframerate	A list of <Positive Integer>	<mode dependent>	0/99	Indicate how many frame rate image sensor outputs in this video mode.
maxfps_mpeg4	A list of <Positive Integer> and "-"	<mode dependent>	0/99	Maximum fps which the device can encoded with MPEG4 on resolutions in this video mode. "-" means not support.
maxfps_mjpeg	A list of <Positive Integer> and "-"	<mode dependent>	0/99	Maximum fps which the device can encoded with MJPEG on resolutions in this video mode. "-" means not support.
maxfps_h264	A list of <Positive Integer> and "-"	<mode dependent>	0/99	Maximum fps which the device can encoded with H.264 on resolutions in this video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter records the frame rate when "videoin_c<n>_cmosfreq"=60 or "videoin_c<n>_modulation"=ntsc * Only available when 'h264' is listed in "capability_videoin_codec".
description	<String[128]>	<mode dependent>	0/99	Description about this mode.

7.28 Customized event script

Group: event_customtaskfile_i<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Custom script identification of this entry.
date	string[4~20]	<blank>	6/6	Date of custom script.
time	string[4~20]	<blank>	6/6	Time of custom script.

7.29 Event setting

Group: **event_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	20	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, recnotify, tampering, visignal, vi, volalarm, temperature, vadp	boot	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "visignal" = Video input signal loss. "recnotify" = Recording notification. "tampering" = Tamper detection. "vi"= Virtual input (Manual trigger) "volalarm" = audio detection. "temperature" = Temperature detection. "vadp" = VADP.
triggerstatus	String[40]	trigger	6/6	The status for event trigger

exttriggerstatus	trigger, normal~trigger, trigger~normal	<blank>	6/6	The status for event DI 1 trigger
di	<integer>	1	6/6	Indicate the source id of di trigger. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	0	6/6	Indicate the source window id of motion detection. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
mdwin0	<integer>	0	6/6	Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.
vi	<integer>	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is "vi". One bit represents one digital input. The LSB indicates VI 0.
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".
weekday	0~127	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)
lowlightcondition	0, 1	1	6/6	Switch on white light LED in low light condition 0 => Do action at all times 1 => Do action in low-light conditions
action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	Duration of the digital output trigger in seconds.
action_goto_enable	<Boolean>	0	6/6	Enable/disable ptz goto preset position on event triggered.
action_goto_name	string[40]	<blank>	6/6	Specify the preset name that ptz goto on event triggered.
action_cf_enable	<Boolean>	0	6/6	Enable or disable sending media to SD card.
action_cf_folder	string[128]	<blank>	6/6	Path to store media.
action_cf_media	NULL, 0~4	<blank>	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	1	6/6	Enable this to create folders by date, time, and hour automatically.
action_cf_backup	<Boolean>	0	6/6	Enable or disable the function that send media to SD card for backup if network is disconnected.
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	NULL, 0~4, 101, 102	<blank>	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.

7.30 Server setting for event action

Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[640]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.
ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.31 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg, temperaturemsg	snapshot	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	Snapshot1_	6/6	Indicate the prefix of the filename. media_i0=> Snapshot1_ media_i1=> Snapshot2_ media_i2=> Snapshot3_ media_i3=> Snapshot4_ media_i4=> Snapshot5_
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
videoclip_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	VideoClipn_ (n: by stream number)	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	0	6/6	Indicates the time for pre-event recording in seconds.

videoclip_maxduration	1 ~ 20	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 6144	3072	6/6	Maximum size of one video clip file in Kbytes.

7.32 Recording

Group: **recording_i**<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.
limitsize	0,1	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	1	6/6	0: Disable recording notification 1: Enable recording notification

notifyserver	0~31	0	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0~i4). bit0 (LSB) = server_i0. bit1 = server_i1. bit2 = server_i2. bit3 = server_i3. bit4 = server_i4. For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.
weekday	0~127	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Start time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	<blank>	6/6	Indicate the prefix of the filename.
cyclesize	200~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	0~	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	cf	6/6	The destination to store the recorded data. "cf" means local storage (CF or SD card). "0" means the index of the network storage.

cffolder	string[128]	NULL	6/6	Folder name.
maxsize	100~2000	100	6/6	Unit: Mega bytes. When this condition is reached, recording file is truncated.
maxduration	60~3600	60	6/6	Uuit: Second When this condition is reached, recording file is truncated.
adaptive_enable	0,1	0	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent	0~9	5	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)
adaptive_postevent	0~10	5	6/6	Indicate when is the adaptive recording stopped after the event trigger point (seconds)

7.33 HTTPS

Group: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	auto	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-3 ~ 1	0	6/6	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.

stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	Asia	6/6	The locality name in the certificate information.
organizationname	string[64]	VIVOTEK Inc.	6/6	Organization name in the certificate information.
unit	string[32]	VIVOTEK Inc.	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek.com	6/6	Common name in the certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.

7.34 Storage management setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
cyclic_enabled	<boolean>	0	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	0	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive integer>	7	6/6	To specify the expired days for automatic clean up.

7.35 Region of interest

Group: **roi_c<0~(n-1)>** for n channel product, and m is the number of streams which support ROI. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
s<0~(m-1)>_home	<coordinate>	0,0	1/6	ROI left-top corner coordinate.
s<0~(m-1)>_size	<window size>	1280x960	1/6	ROI width and height. The width value must be multiples of 16 and the height value must be multiples of 8

7.36 ePTZ setting

Group: **eptz_c<0~(n-1)>** for n channel product. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
osdzoom	<boolean>	1	1/4	Indicates multiple of zoom in is "on-screen display" or not
smooth	<boolean>	1	1/4	Enable the ePTZ "move smoothly" feature
tiltspeed	-5 ~ 5	0	1/7	Tilt speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
panspeed	-5 ~ 5	0	1/7	Pan speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
zoomspeed	-5 ~ 5	0	1/7	Zoom speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
autospeed	1 ~ 5	1	1/7	Auto pan/patrol speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

Group: **eptz_c<0~(n-1)>_s<0~(m-1)>** for n channel product and m is the number of streams which support ePTZ. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
patrolseq	string[120]	<blank>	1/4	The patrol sequence of ePTZ. All the patrol position indexes will be separated by ","
patroldwelling	string[160]	<blank>	1/4	The dwelling time (unit: second) of each patrol point, separated by ",".
preset_i<0~19>_name	string[40]	<blank>	1/7	Name of ePTZ preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)
preset_i<0~19>_pos	<coordinate>	<blank>	1/7	Left-top corner coordinate of the preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)

preset_i<0~19>_size	<window size>	<blank>	1/7	Width and height of the preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)

7.37 Exposure window setting per channel

Group: **exposurewin_c<0~(n-1)>** for n channel products

(capability_videoin_supportexpwin = 1)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	auto, custom, blc	auto	4/4	The mode indicates how to decide the exposure. auto: Use full view as the only one exposure window. custom: Use inclusive and exclusive window. blc: Use BLC.
win_i<0~9>_enable	<boolean>	0	4/4	Enable or disable the window.
win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive. 1: Indicate inclusive.
win_i<0~9>_home	<coordinate>	110,90	4/4	Left-top corner coordinate of the window.
win_i<0~9>_size	<window size>	100x75	4/4	Width and height of the window.

Group: **exposurewin_c<0~(n-1)>_profile** for m profile and n channel product

(capability_videoin_supportexpwin = 1)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
i<0~(m-1)>_mode	auto, custom, blc	auto	4/4	The mode indicates how to decide the exposure. auto: Use full view as the only one exposure window. custom: Use inclusive and exclusive window. blc: Use BLC.
i<0~(m-1)>_win_i<0~9>_enable	<boolean>	0	4/4	Enable or disable the window.
i<0~(m-1)>_win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive. 1: Indicate inclusive.
i<0~(m-1)>_win_i<0~9>_home	<coordinate>	110,90	4/4	Left-top corner coordinate

				of the window.
i<0~(m-1)>_win_i<0~9>_size	<window size>	100x75	4/4	Width and height of the window.

8. Useful Functions

Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>]
```

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1 .

Request:

http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

di1=1\r\n

Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: <*length*>\r\n

\r\n

[do0=<state>]\r\n

[do1=<state>]\r\n

[do2=<state>]\r\n

[do3=<state>]\r\n

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

```
\r\n
do1=1\r\n
```

Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available resolution>	0	The resolution of the image.
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	<product dependent>	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][…][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Logs

Note: This request require Administrator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/syslog.cgi

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upgrade.cgi

Post data:

fimage=<file name>[&return=<return page>]\r\n \r\n <multipart encoded form data>

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

ePTZ Camera Control (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value> [&move=<value>] – Move home, up, down, left, right [&auto=<value>] – Auto pan, patrol [&zoom=<value>] – Zoom in, out [&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick [&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick [&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image (Move the center of image to the coordination (x,y) based on resolution or videosize.) [[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>]] – Set speeds [&return=<return page>]

Example:

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100&videosize=640x480&resolution=640x480&stretch=0

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
vx	<integer>	The direction of movement, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system. 1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.

speedapp	1 ~ 5	Set the auto pan/patrol speed.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

ePTZ Recall (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>&recall=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
recall	Text string less than 40 characters	One of the present positions to recall.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

ePTZ Preset Locations (capability.eptz > 0)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value>[&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.

addpos	<Text string less than 40 characters>	Add one preset location to the preset list.
delpos	<Text string less than 40 characters>	Delete preset location from the preset list.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<*ipaddress*>&end=<*ipaddress*>][&index=<*value*>]
[&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

IP Filtering for ONVIF

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Event/Control HTTP Tunnel Channel (capability. evctrlchannel > 0)

Note: This request requires Administrator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/admin/ctrlevent.cgi

GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

```
------------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

Get SDP of Streams

Note: This request requires Viewer access privileges.
Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

"m" is the stream number.
"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.
You can get the SDP by HTTP GET.
When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

Storage managements (capability.storage.dbenabled > 0)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>…]

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*.

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.

mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'
isLocked	<boolean>	Optional. Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is "YYYY-MM-DD HH:MM:SS" Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply "TO" operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'

Command: **delete**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8

Command: **update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript

Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate] Where "state" is 0, 1. "0" means inactive or normal state while "1" means active or triggered state. Where "nstate" is next state after duration.	Ex: vi0=1 Setting virtual input 0 to trigger state
		Ex: vi0=0(200)1 Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state. Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	<return page>	Redirect to the page *<return page>* after the request is completely assigned. The *<return page>* can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

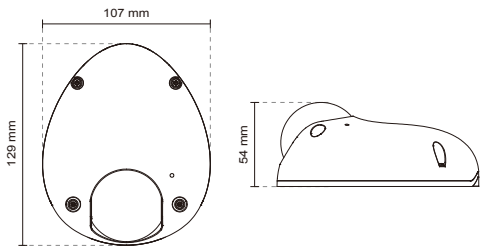
Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. setvi.cgi?vi3=0 VI index is out of range. setvi.cgi?vi=1 No VI index is specified.
503	The resource is unavailable, ex. Virtual input is waiting for next state. Examples: setvi.cgi?vi0=0(15000)1 setvi.cgi?vi0=1 Request 2 will not be accepted during the execution time(15 seconds).

Technical Specifications

Model	MD8531H
System Information	
CPU	Multimedia SoC (System-on-Chip)
Flash	128 MB
RAM	256 MB
Camera Features	
Image Sensor	1/3" Progressive CMOS
Maximum Resolution	1280x960
Lens Type	Fixed-focal
Focal Length	f = 3.6mm (MD8531H-F3) f = 4.2mm (MD8531H-F4)
Aperture	F1.8
Field of View	MD8531H-F3: 80˚(Horizontal) 57˚(Vertical) 103˚(Diagonal) MD8531H-F4: 68˚(Horizontal) 50˚(Vertical) 90˚(Diagonal)
Shutter Time	1/5 sec. to 1/32,000 sec.
WDR Technology	WDR Pro
Minimum Illumination	0.4 Lux @ F1.8, 30 IRE(Color)
Pan/tilt/zoom Functionalities	ePTZ: 48x digital zoom (4x on IE plug-in,12x built in)
On-board Storage	MicroSD/SDHC/SDXC card slot
Video	
Compression	H.264, MPEG-4 & MJPEG
Maximum Frame Rate	H.264: 30fps @ 1280x960, 30fps @ 960x1280 MPEG-4: 30fps @ 1280x960, 30fps @ 960x1280 MJPEG: 30 fps @ 1280x960, 30fps @ 960x1280
Maximum Streams	4 simultaneous streams
S/N Ratio	Above 60 dB
Dynamic Range	120dB
Video Streaming	Adjustable resolution, quality and bitrate Video rotation
Image Settings	Adjustable image size, quality and bit rate Time stamp, text overlay, flip & mirror Configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks Scheduled profile settings, 3D Noise Reduction
Audio	
Audio Capability	Two-way audio (full duplex)
Compression	G.711, G.726
Interface	Built-in microphone Audio output
Effective Range	5 meters
Network	
Users	Live viewing for up to 10 clients
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X, UDP, ICMP
Interface	10Base-T/100 BaseTX Ethernet (RJ-45)
ONVIF	Supported, specification available at www.onvif.org
Intelligent Video	
Video Motion Detection	Triple-window video motion detection

Alarm and Event	
Alarm Triggers	Video motion detection, manual trigger, digital input, periodical trigger, system boot, recording notification, camera tampering detection, temperature detection, audio detection
Alarm Events	Event notification using HTTP, SMTP, FTP and NAS server File upload via HTTP, SMTP, FTP and NAS server
General	
Connectors	RJ-45 for Network/PoE connection Audio output Digital output*1 Digital input*1
LED Indicator	System power and status indicator
Power Input	IEEE 802.3af PoE Class 1
Power Consumption	Max. 3.8W (PoE)
Dimensions	129 mm (D) x 107 mm (W) x 54 mm (H)
Weight	Net: 392g
Casing	Weather-proof IP66-rated housing Vandal-proof IK10-rated housing
Safety Certifications	CE, LVD, FCC Class A, VCCI, C-Tick, EN50155
Operating Temperature	Starting Temperature: -25˚C ~ 55˚C (-13˚F ~ 131˚F) Working Temperature: -25˚C ~ 55˚C (-13˚F ~ 131˚F)
Warranty	36 months
System Requirements	
Operating System	Microsoft Windows 8/7/Vista/XP/2000
Web Browser	Mozilla Firefox 7~10 (streaming only) Internet Explorer 7/8/9/10
Other Players	VLC: 1.1.11 or above QuickTime: 7 or above
Included Accessories	
CD	User's manual, quick installation guide, Installation Wizard 2, ST7501 32-channel recording software
Others	Quick installation guide, screwdriver, alignment sticker, Softeware CD

Dimensions



Compatible Accessories

PoE Kits

POE-IJ-1748NDN
PoE injector, 802.3af compliant

All specifications are subject to change without notice. Copyright © VIVOTEK INC. All rights reserved.

Distributed by:

VIVOTEK
EEEE.VIVOTEK.COM

Ver 1.0

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho,
New Taipei City, 235, Taiwan, R.O.C.
T: +886-2-82455282 F: +886-2-82455532
E: sales@vivotek.com

VIVOTEK USA
2050 Ringwood Avenue,
San Jose, CA 95131
T: 408-773-8686 F: 408-773-8298
E: salesusa@vivotek.com

VIVOTEK Europe
Busplein 36, 1315KV, Almere,
The Netherlands
T: +31(0)36-5389-149 F: +31(0)36-5389-111
E: saleseurope@vivotek.com

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

■ Reorient or relocate the receiving antenna.

■ Increase the separation between the equipment and receiver.

■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

■ Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準にづくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.